Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»

# КОМПЛЕКС ЭЛЕКТРОННЫХ МАТЕРИАЛОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ»

Выпускная квалификационная работа
по направлению подготовки 44.03.04 Профессиональное обучение
(по отраслям)
профилю подготовки «Информатика и вычислительная техника»
профилизации «Информационная безопасность»

Идентификационный номер ВКР: 304

Екатеринбург 2018

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

К ЗАЩИТЕ ДОПУСКАЮ
Заведующая кафедрой ИС
_____ Н. С. Толстова
«____» _____ 2018 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

# КОМПЛЕКС ЭЛЕКТРОННЫХ МАТЕРИАЛОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ»

Исполнитель:
обучающийся группы № ИБ-401 В. А. Титов
Руководитель:
канд. пед. наук, доцент И. А. Суслова
Нормоконтролер: Т. В. Рыжкова

Екатеринбург 2018

# АННОТАЦИЯ

Выпускная квалификационная работа состоит из комплекса электронных материалов «Информационная безопасность в социальных сетях» и пояснительной записки на 49 страницах, содержащей 35 рисунков, 31 источник литературы, а также 1 приложений на 49 страницах.

Ключевые слова: ЭЛЕКТРОННЫЕ МАТЕРИАЛЫ, СОЦИАЛЬНАЯ СЕТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ВИДЕОМАТЕРИАЛЫ, УГРОЗА

**Титов, В. А.,** Комплекс электронных материалов «Информационная безопасность в социальных сетях»**:** выпускная квалификационная работа / В. А. Титов; Рос. гос. проф.-пед. ун-т, Ин-т инж.-пед. образования, Каф. информ. систем и технологий. — Екатеринбург, 2017. — 49 с.

Объектом исследования выпускной квалификационной работы является процесс обучения информационной безопасности в социальных сетях.

Предметом исследования выпускной квалификационной работы является интернет-статьи по информационной безопасности в социальных сетях.

Цель выпускной квалификационной работы — разработать комплекс электронных материалов «Информационная безопасность в социальных сетях». Отличительной особенностью данного комплекса электронных материалов «Информационная безопасность в социальных сетях» является то, что пользователи могут изучать видеоматериалы в любое доступное для них время, а также с любого доступного устройства, благодаря оптимизированной мобильной версии продукта. Также ко всем озвученным видеоматериалам прилагается текстовая версия видеоматериала, в которой раскрывается ключевая проблема в полном объеме.

# СОДЕРЖАНИЕ

# ВВЕДЕНИЕ

В настоящее время все быстрее и больше информационные технологии входят в образ жизни людей, с целью обеспечения более простого и комфортного взаимодействия с компьютером.

На сегодняшний день информационные технологии развились до такой степени автономности, что пользователи даже не замечают, на сколько быстро и качественно производится взаимодействие в сети Интернет. В процессе работы в сети Интернет, используются методы сбора, обработки, хранении, преобразовании, и распределения больших объемов информации, будь это просто переход на сайт, или же оплаченная покупка в магазине (транзакция), все это неотъемлемая часть нашей жизни.

Поэтому, под вопрос безопасности, и корректной сохранности информации, встает главная тема обсуждения нашего времени — защита персональных данных. Не для никого не секрет, что в современном мире невозможно обойтись без социальных сетей. На данный момент каждый человек который связанный с компьютером, зарегистрирован как минимум в одной социальной сети.

Как показывает практика, многие люди не задумываются о безопасности персональных данных, ведь при регистрации в социальной сети, для продолжения регистрации пользователю необходимо указать информацию о себе, такую как имя, фамилию, отчество, дата рождения, город рождения, город проживания, адрес проживания, номер сотового телефона, e-mail, и в добавок к этому некоторые социальные сети требуют от пользователя, что бы он загрузил в профиль, свое реальное фото.

Хочется также отметить, что социальные сети не только хранят и обрабатывают персональные данные пользователей, но и содержат различную провокационную, а чаще всего ложную информацию, без должной фильтрации содержимого контента той или иной социальной сети.

Не стоит забывать о том, что в социальных сетях имеются мошенники, которые под видом обычных пользователей входят в доверие обычного пользователя, тем самым совершают хищение, будь то моральных, финансовых, или же информационных ценностей, для личной выгоды.

Информационная безопасность социальных сетях является актуальной, потому что, казалось бы, при банальной регистрации в социальной сети, пользователь сам указывает о себе персональные данные. Однако если обычный пользователь пренебрег настройками отображения персональной информации в своем профиле, то другой пользователь с негативным умыслом может скопировать необходимую злоумышленнику информацию, воспользовавшись стандартным поиском в социальной сети.

Однако в социальных сетях при правильном ее использовании, это довольно хорошее средство массовой информации. Полезно узнавать что-то новое, читать интересующие пользователей статьи, участвовать в той или иной дискуссии.

Объект исследования — процесс обучения информационной безопасности в социальных сетях.

Предмет исследования — материалы по информационной безопасности в социальных сетях.

Цель исследования — разработать комплекс электронных материалов «Информационная безопасность в социальных сетях».

Для достижения цели необходимо решить следующие задачи:

- проанализировать литературу и интернет-источники по теме «Информационная безопасность в социальных сетях»;
- проанализировать требования, предъявляемые к пользовательскому интерфейсу;
- разработать видеоматериалы по теме «Информационная безопасность в социальных сетях»;
- спроектировать структуру и реализовать интерфейс, функционал и наполнение комплекса электронных материалов.

# 1 АНАЛИЗ ЛИТЕРАТУРЫ ПО ПРОБЛЕМЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ»

## 1.1 Основные виды рисков в социальных сетях

В настоящее время социальные сети все больше выполняют цель оперативного информирования своей аудитории. И за частую пользователи социальных сетей становятся не только потребителями информации, но и главным ее источником. Но не смотря на потенциал и скорость распространения информации в социальных сетях, данные социальные сети все чаще оказываются в такой ситуации, в которой источники информации становятся неконтролируемыми, и это внушает все большее опасения. Одним из вредного воздействия социальных сетей на человека является провокационный контент, направленный на разрушение общечеловеческих ценностей, также следует не только нарушение их личностных поведенческие стратегии, но и модель поведения человека в обществе в целом, все это базируется на трех основных определяющих понятиях, такие как, моральные принципы, поведение, и нравственные ценности. В Российской Федерации наиболее популярный и самая посещаемая социальная сеть является «ВКонтакте». Самые большие риски в данной социальной сети несут группы, и публичные страницы, доступ к которым полностью открыт для ознакомления. Следует отметить что в социальной сети «ВКонтакте» Практически во всем группах и публичных страницах, состоит как минимум сотня пользователей, но чаще всего эти цифры достигают несколько миллионов пользователей.

На примере социальной сети «ВКонтакте» выявлены и охарактеризованы основные виды рисков.

Обычный пользователь сталкивается достаточно часто:

- публикации недостоверной информации в группах и публичных страницах с дальнейшим ее распространением. Данный риск является одним из самых распространённых в социальных сетях. Обычно это касается от искажения новостей до неправильного указания автора на ту или иную информацию, либо цитату;
- непроверенной информации о какой-либо продаже товара, либо предоставление услуг непосредственно от сомнительных источников информации в социальных сетях. И как показывает статистика и практика, это заканчивается тем, что это продажа известных брендов под заказ, которые чаще всего оказываются подделкой. Мало того, что пользователь приобрел товар за некую сумму в конце концов получает товар, либо не соответствующий описанию и характеристикам, либо пользователь в конечном итоге вообще не получает товар;
- наткнуться на нежелательный контент, например, фото, видео и иные материалы несущее эротический и порнографический информационный характер, предназначенный в первую очередь для пользователей возраст которых более восемнадцати лет, тем более эротическая и порнографическая информация находится в свободном для пользователей доступе. Также это могут быть фотографии, сделанные на реальных мероприятиях, также хранящихся в открытом доступе, сделанные, например, в клубах, следует помнить о том, что это могут быть порнографические ролики, снятые в рамках, не только домашнего видео, но и в специальных проектах. В основном эту информацию можно найти в тех же группах и публичных страницах;
- столкнуться с пропагандой нездорового образа жизни, что встречается крайне часто. Например, пропаганда незаконного употребления наркотических веществ, алкогольных напитков, употребление табачной продукции. Высоки риски попасть под давление сверстников, которые сами пропагандируют незаконное употребление наркотических веществ, алкогольных

напитков, употребление табачной продукции, путем публикации фото на котором производится данная пропаганда;

- попасть под пропаганду, представляющую собой угрозы для здоровья, а также жизни пользователей социальной сети. Например, пропаганда, призывающая к суициду, также пропаганда нездорового образа жизни как мода на анорексию;
- пропаганды употребления в речевых словосочетаниях нецензурного лексикона. Конечно она так или иначе присутствует в личных сообщениях пользователей, но одно дело, когда это личная переписка, а другое, когда, это выставляется на всеобщее обозрение, под видом того, что это «нормально»;
- встретить подозрительное предложение на трудоустройство из непроверенного сомнительного источника. Обычно данный психологический метод используется на пользователях социальной сети, которые желающих разбогатеть, не покидая своего дома. В основном используются методы речевого воздействия на пользователя социальной сети, затем уже оказывается психологическое воздействие на пользователя социальной сети;
- быть взломанным, когда вся ваша личная информация находится в руках мошенника, или, например, от вашего имени распространяют ложную информацию или какую-либо пропаганду, также существует рассылка спама другим пользователям социальной сети, вся эта информация, рассылаемая от вашего имени может выходить за рамки этики и закона, либо получение денежных средств незаконными способами;
- учувствовать в различных розыгрышах и конкурсах, которые обычно являются обманом для всех пользователей социальной сети, участвовавших в данной афере. На практике скорее всего вы не получите приза, зато есть риск перехода по вредоносной ссылке, переходя по ссылке есть высокой шанс того, что ваше устройство будет заражено вредоносным программным обеспечением, с целью уничтожения, изменения, а также кражи личных данных;

- неправильного формирования культуры и ценностей пользователей в социальной сети. Под эту категорию рисков входят как, семейные и религиозные ценности, нормы этики, так и морали и т.д.;
- попасть под пропаганду насилия и жестокого обращения с людьми. В качестве метода используются видеоматериалы, на которых демонстрируются жестокое обращение с животными, издевательство над инвалидами, унижение моральных ценностей, издевательство над женщинами, публичное насилие, что также находится в открытом доступе для любого пользователя социальной сети;
- встретить пропаганду разжигания конфликтов между несколькими различными социальными группами, такие как разжигание межнациональных, религиозных конфликтов;
- попасть под пропаганду запрещенных законодательством, направлений, организаций, и группировок, созданные с целью экстремизма, также и запрещенные религиозные сообщества и т.д.

Это далеко не полный список всех рисков, встречающихся пользователям на просторах социальных сетей. Однако можно утверждать, что данные риски одни из самых распространенных рисков, встречающихся пользователям социальных сетей. И это касается не только детей, находящихся на этапе формирования мировоззрения, моральных ценностей, и жизненных установок, но и сформировавшихся как личность людей чьи психологические состояния являются нестабильными, которые смогут сделать то или иное решение или поступок, будучи находившимся под психологическим воздействием мошенников. Таким образом, все риски можно разделить на: информационные, материальные, морально-нравственные, психологические, и экзистенциальные.

## 1.2 Обзор литературы и интернет-источников

### 1.2.1 Обзор печатных источников

Перед началом работы, было проанализировано большое количество информации представленной как Интернете, так и в печатном виде. После изучения всех возможных материалов, можно было прийти к выводу, что в русскоязычном варианте печатных источников нет полной информации на тему «Информационная безопасность в социальных сетях». К сожалению более раскрытая информация предлагается в иностранных печатных изданиях.

В книге «Social Media Security» [30] (рисунок 1) описывается проблема пренебрежения персональных данных, при регистрации в социальных сетях. Раскрывается проблема несерьезного отношения к предоставляемым персональным данным, а так незнание о стандартных настройках приватности в социальных сетях, хотя в этом нет ничего сложного, необходимо всего лишь уделить настройкам приватности 5 — 10 минут, но большинство пользователей этим пренебрегают. Все потому что на первый взгляд для обычного пользователя стандартные настройки приватности обеспечивают простоту использования социальных сетей, но такая простота, негативно влияет на отображение персональных данных пользователей. Также в книге говорится о различных способах разграничения видимой информации о персональных данных, это позволяет оградить некоторую информацию от других пользователей социальной сети. В книге присутствует описание видов угроз, способов защиты персональных данных в сети Интернет.

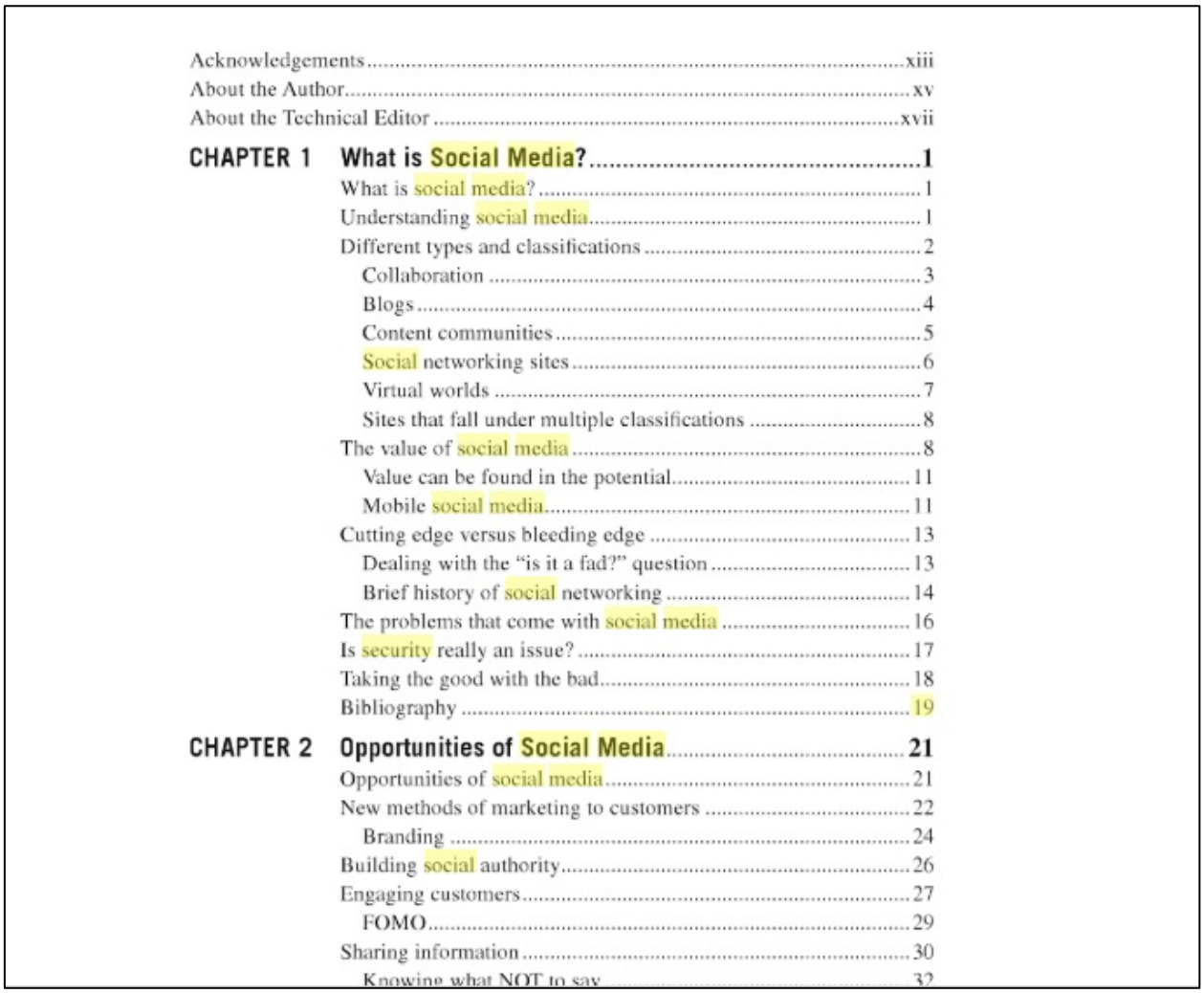




Рисунок 1 — Внешний вид оглавления

Эта книга (рисунок 2) поможет организации понять риски, существующие в социальных сетях, и предоставить структуру, охватывающую политику, обучение и технологию для решения этих проблем, и смягчения рисков, которые могут быть использованы для использования социальных сетей в их организации. В книге также признается, что многие организации уже подвергли себя риску больше, чем думают в социальных сетях, и предлагают стратегии для его устранения, чтобы вернуть контроль.

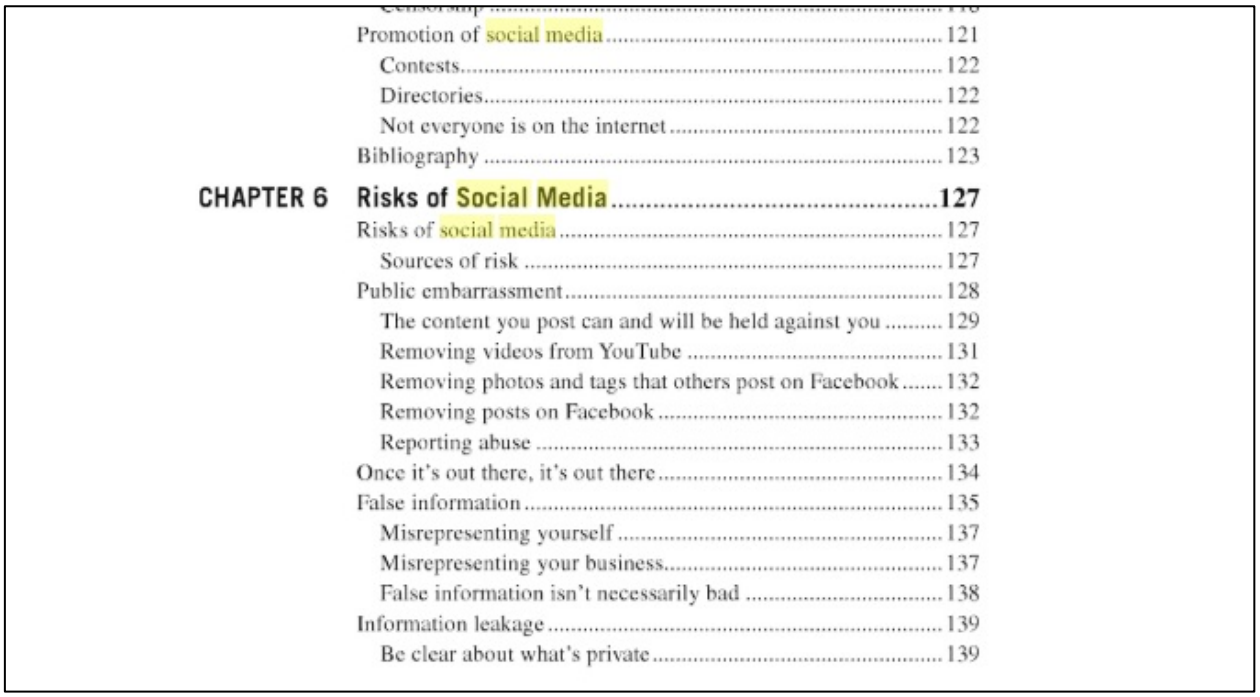



Рисунок 2 — Оглавление

Книга «Security and Privacy in Social Networks» [31] (рисунок 3) о том, как создавались социальные сети, в области они развивались, и что в конечном итоге мы имеем в наше время. Книга раскрывает проблемы зависимости от социальных сетей, о том сколько в среднем количестве времени проводит пользователь в социальных сетях, а также как он сам пополняет информацию о своих персональных данные в своем профиле, тем самым, не задумываясь о защите своих персональных данных. В книге рассматриваются шаблоны поведения пользователей в социальных сетях, и о том, как пользователи вели дискуссию, и сами того не понимая выдавали о себе конфиденциальные данные. Книга описывает как склонны пользователя социальной сети игнорировать меры предосторожности и наивно полагаться на ложное чувство близости и неприкосновенности частной жизни, даже не осознавая весь ущерб от происходящего. Исходя из этого в книге по мнению автора описывается неоценимая угроза безопасности персональных данных в социальных сетях.

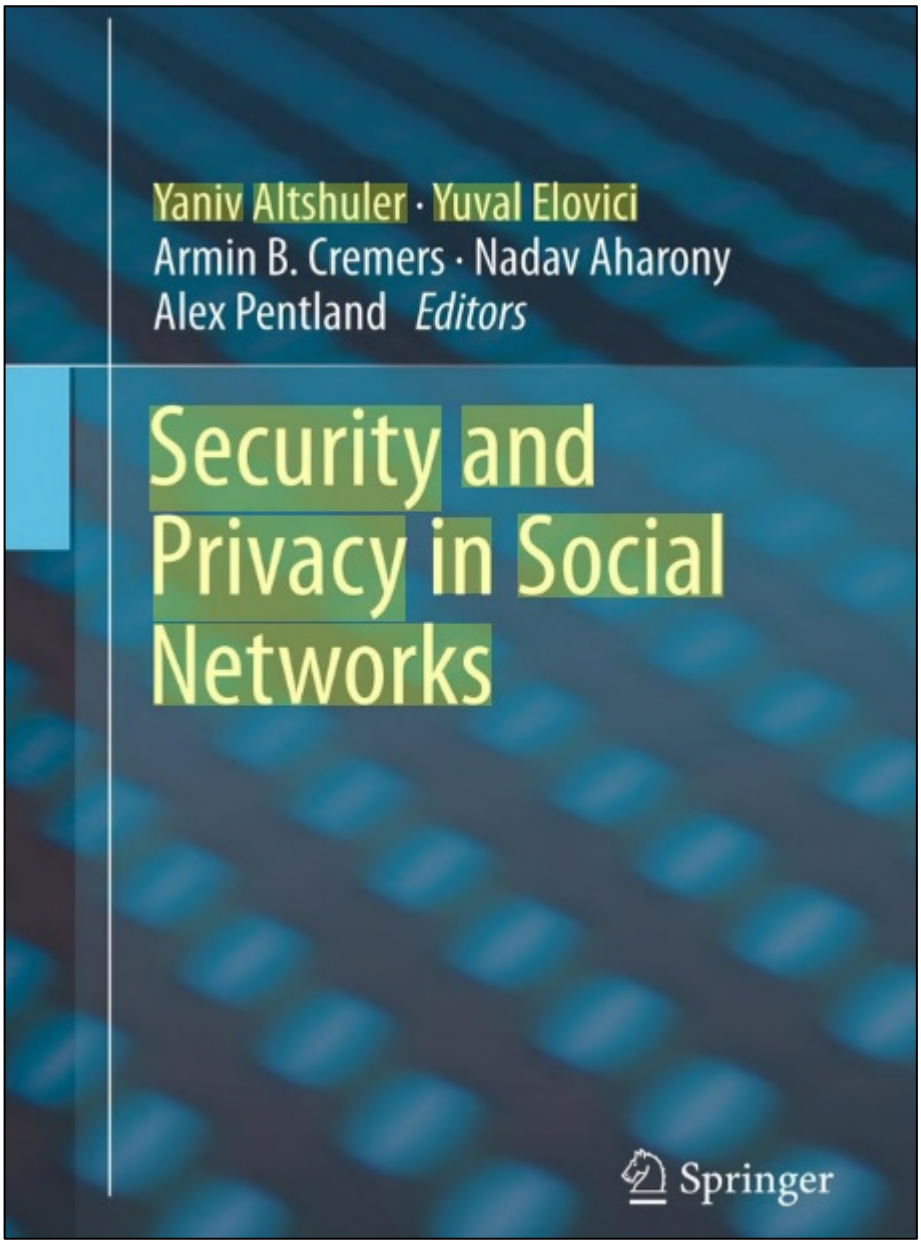



Рисунок 3 — Внешний вид обложки

### 1.2.2 Обзор интернет-источников

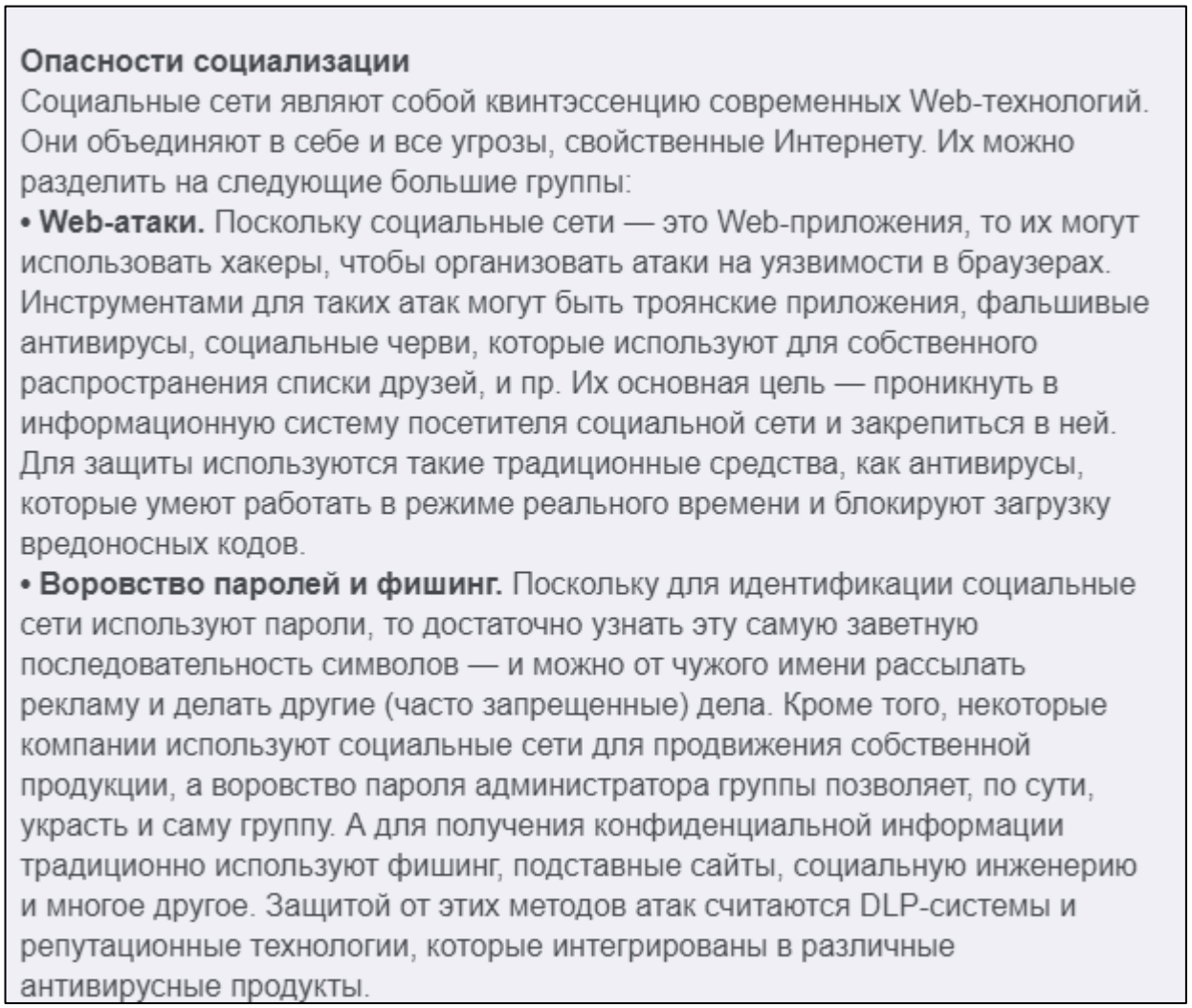
Работая с различными интернет-источниками, необходимо выделить сайты:

В статье «Защита персональных данных в социальных сетях» [12] (рисунок 4) описываются методы защиты, такие как:

- используйте механизмы безопасности, предоставляемые социальными сетями;

- используйте общие механизмы безопасности, не привязанные к социальным сетям;
- пребывая в социальной сети, совершайте действия, не угрожающие вашим персональным данным.

Упоминается о поиске в социальных сетях, который дает возможность любому пользователю получить определенный перечень информации о конкретном профиле.



**Опасности социализации**

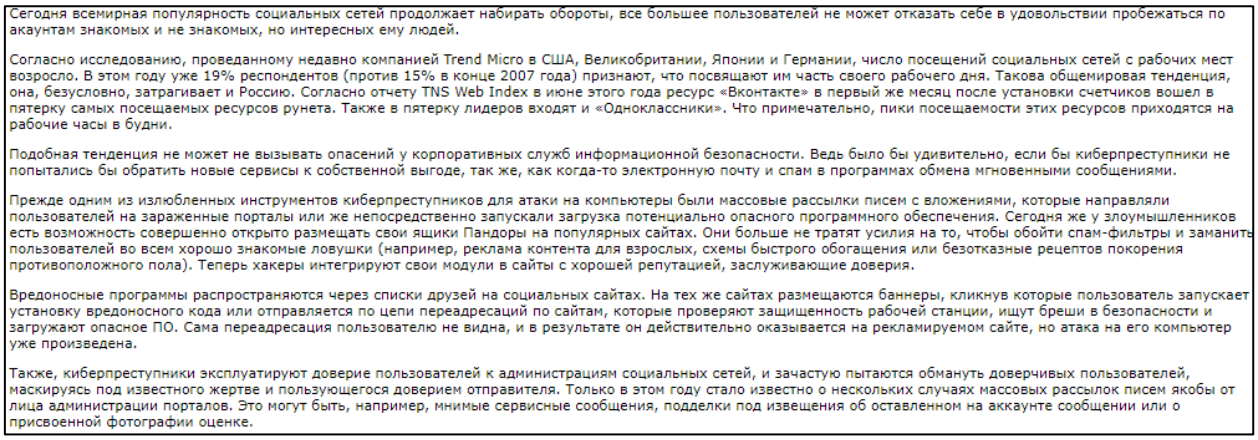
Социальные сети являют собой квинтэссенцию современных Web-технологий. Они объединяют в себе и все угрозы, свойственные Интернету. Их можно разделить на следующие большие группы:

• **Web-атаки.** Поскольку социальные сети — это Web-приложения, то их могут использовать хакеры, чтобы организовать атаки на уязвимости в браузерах. Инструментами для таких атак могут быть троянские приложения, фальшивые антивирусы, социальные черви, которые используют для собственного распространения списки друзей, и пр. Их основная цель — проникнуть в информационную систему посетителя социальной сети и закрепиться в ней. Для защиты используются такие традиционные средства, как антивирусы, которые умеют работать в режиме реального времени и блокируют загрузку вредоносных кодов.

• **Воровство паролей и фишинг.** Поскольку для идентификации социальные сети используют пароли, то достаточно узнать эту самую заветную последовательность символов — и можно от чужого имени рассылать рекламу и делать другие (часто запрещенные) дела. Кроме того, некоторые компании используют социальные сети для продвижения собственной продукции, а воровство пароля администратора группы позволяет, по сути, украсть и саму группу. А для получения конфиденциальной информации традиционно используют фишинг, подставные сайты, социальную инженерию и многое другое. Защитой от этих методов атак считаются DLP-системы и репутационные технологии, которые интегрированы в различные антивирусные продукты.

Рисунок 4 — Скриншот источника

В статье «Угрозы социальных сетей» [29] (рисунок 5) описается насколько велика угроза социальных сетей, модели угроз, а также средства защиты.


Сегодня всемирная популярность социальных сетей продолжает набирать обороты, все большее пользователей не может отказать себе в удовольствии пробежаться по акаунтам знакомых и не знакомых, но интересных ему людей.

Согласно исследованию, проведанному недавно компанией Trend Micro в США, Великобритании, Японии и Германии, число посещений социальных сетей с рабочих мест возросло. В этом году уже 19% респондентов (против 15% в конце 2007 года) признают, что посвящают им часть своего рабочего дня. Такова общемировая тенденция, она, безусловно, затрагивает и Россию. Согласно отчету TNS Web Index в июне этого года ресурс «Вконтакте» в первый же месяц после установки счетчиков вошел в пятерку самых посещаемых ресурсов рунета. Также в пятерку лидеров входят и «Одноклассники». Что примечательно, пики посещаемости этих ресурсов приходятся на рабочие часы в будни.

Подобная тенденция не может не вызывать опасений у корпоративных служб информационной безопасности. Ведь было бы удивительно, если бы киберпреступники не попытались бы обратить новые сервисы к собственной выгоде, так же, как когда-то электронную почту и спам в программах обмена мгновенными сообщениями.

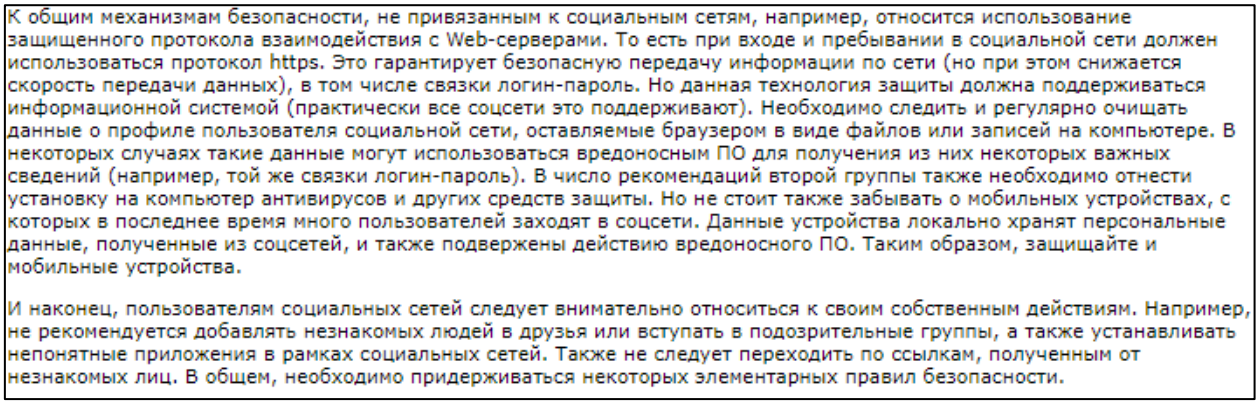
Прежде одним из излюбленных инструментов киберпреступников для атаки на компьютеры были массовые рассылки писем с вложениями, которые направляли пользователей на зараженные порталы или же непосредственно запускали загрузка потенциально опасного программного обеспечения. Сегодня же у злоумышленников есть возможность совершенно открыто размещать свои ящики Пандоры на популярных сайтах. Они больше не тратят усилия на то, чтобы обойти спам-фильтры и заманить пользователей во всем хорошо знакомые ловушки (например, реклама контента для взрослых, схемы быстрого обогащения или безотказные рецептов покорения противоположного пола). Теперь хакеры интегрируют свои модули в сайты с хорошей репутацией, заслуживающие доверия.

Вредоносные программы распространяются через списки друзей на социальных сайтах. На тех же сайтах размещаются баннеры, кликнув которые пользователь запускает установку вредоносного кода или отправляется по цепи переадресаций по сайтам, которые проверяют защищенность рабочей станции, ищут бреши в безопасности и загружают опасное ПО. Сама переадресация пользователю не видна, и в результате он действительно оказывается на рекламируемом сайте, но атака на его компьютер уже произведена.

Также, киберпреступники эксплуатируют доверие пользователей к администрациям социальных сетей, и зачастую пытаются обмануть доверчивых пользователей, маскируясь под известного жертве и пользующегося доверием отправителя. Только в этом году стало известно о нескольких случаях массовых рассылок писем якобы от лица администрации порталов. Это могут быть, например, мнимые сервисные сообщения, подделки под извещения об оставленном на аккаунте сообщении или о присвоенной фотографии оценке.

Рисунок 5 — Внешний вид скриншота сайта

В статье «Социальные сети как угроза корпоративной информационной безопасности» [27] (рисунок 6) описывается как злоумышленники получают несанкционированный доступ к персональным данным обычных пользователей. Описание алгоритмов работы защиты социальных сетей.


К общим механизмам безопасности, не привязанным к социальным сетям, например, относится использование защищенного протокола взаимодействия с Web-серверами. То есть при входе и пребывании в социальной сети должен использоваться протокол https. Это гарантирует безопасную передачу информации по сети (но при этом снижается скорость передачи данных), в том числе связки логин-пароль. Но данная технология защиты должна поддерживаться информационной системой (практически все соцсети это поддерживают). Необходимо следить и регулярно очищать данные о профиле пользователя социальной сети, оставляемые браузером в виде файлов или записей на компьютере. В некоторых случаях такие данные могут использоваться вредоносным ПО для получения из них некоторых важных сведений (например, той же связки логин-пароль). В число рекомендаций второй группы также необходимо отнести установку на компьютер антивирусов и других средств защиты. Но не стоит также забывать о мобильных устройствах, с которых в последнее время много пользователей заходят в соцсети. Данные устройства локально хранят персональные данные, полученные из соцсетей, и также подвержены действию вредоносного ПО. Таким образом, защищайте и мобильные устройства.

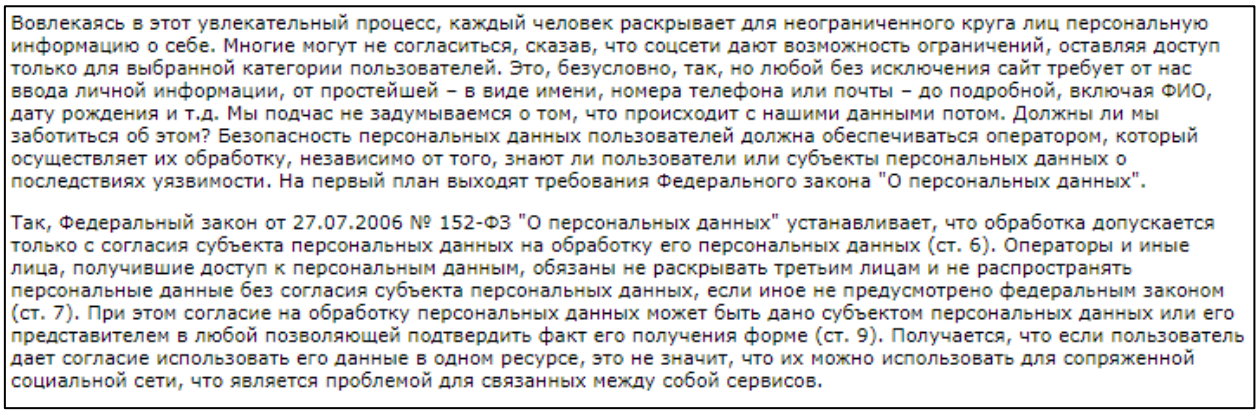
И наконец, пользователям социальных сетей следует внимательно относиться к своим собственным действиям. Например, не рекомендуется добавлять незнакомых людей в друзья или вступать в подозрительные группы, а также устанавливать непонятные приложения в рамках социальных сетей. Также не следует переходить по ссылкам, полученным от незнакомых лиц. В общем, необходимо придерживаться некоторых элементарных правил безопасности.

Рисунок 6 — Внешний вид наполнения сайта

В статье «Защита персональных данных в социальных сетях» [13] (рисунок 7) описываются проблемы защиты персональных данных, Политика конфиденциальности в социальных сетях.

Также рассматривается тема безопасности с точки зрения «Успевает ли закон за ростом и трансформацией социальных сетей и в полной ли мере он отражает все потребности этой сферы?»

Статья содержит описание, каким образом и где хранятся персональные данные об пользователе.



Вовлекаясь в этот увлекательный процесс, каждый человек раскрывает для неограниченного круга лиц персональную информацию о себе. Многие могут не согласиться, сказав, что соцсети дают возможность ограничений, оставляя доступ только для выбранной категории пользователей. Это, безусловно, так, но любой без исключения сайт требует от нас ввода личной информации, от простейшей – в виде имени, номера телефона или почты – до подробной, включая ФИО, дату рождения и т.д. Мы подчас не задумываемся о том, что происходит с нашими данными потом. Должны ли мы заботиться об этом? Безопасность персональных данных пользователей должна обеспечиваться оператором, который осуществляет их обработку, независимо от того, знают ли пользователи или субъекты персональных данных о последствиях уязвимости. На первый план выходят требования Федерального закона "О персональных данных".

Так, Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" устанавливает, что обработка допускается только с согласия субъекта персональных данных на обработку его персональных данных (ст. 6). Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом (ст. 7). При этом согласие на обработку персональных данных может быть дано субъектом персональных данных или его представителем в любой позволяющей подтвердить факт его получения форме (ст. 9). Получается, что если пользователь дает согласие использовать его данные в одном ресурсе, это не значит, что их можно использовать для сопряженной социальной сети, что является проблемой для связанных между собой сервисов.

Рисунок 7 — Внешний вид основного наполнения сайта

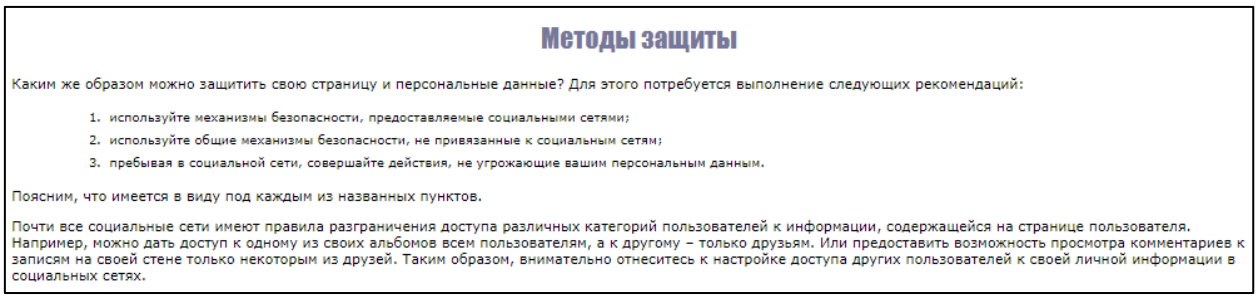
В статье «безопасность персональных данных в социальных сетях» [7] (рисунок 8) рассматривается способы защиты персональных данных.

Также описываются меры безопасности в интернете.

Обоснованное мнение влияния на жизнь с точки зрения:

- экономики;
- социума;
- политики.

А также актуальность проблемы в наше время.



**Методы защиты**

Каким же образом можно защитить свою страницу и персональные данные? Для этого потребуется выполнение следующих рекомендаций:

1. используйте механизмы безопасности, предоставляемые социальными сетями;
2. используйте общие механизмы безопасности, не привязанные к социальным сетям;
3. пребывая в социальной сети, совершайте действия, не угрожающие вашим персональным данным.

Поясним, что имеется в виду под каждым из названных пунктов.

Почти все социальные сети имеют правила разграничения доступа различных категорий пользователей к информации, содержащейся на странице пользователя. Например, можно дать доступ к одному из своих альбомов всем пользователям, а к другому – только друзьям. Или предоставить возможность просмотра комментариев к записям на своей стене только некоторым из друзей. Таким образом, внимательно отнеситесь к настройке доступа других пользователей к своей личной информации в социальных сетях.

Рисунок 8 — Внешний вид статьи

В статье «Как именно хакеры взламывают аккаунты в социальных сетях» [15] (рисунок 9) описываются методы взлома аккаунтов в социальных сетях, их мотивы и причины.

Описываются элементарные методы предотвращения взлома аккаунты, необходимые средства защиты, а также минимальные советы по обеспечению безопасности персональных данных.

**ДЛЯ ХАКЕРОВ ВЗЛОМ АККАУНТОВ — ОДНО ИЗ САМЫХ УВЛЕКАТЕЛЬНЫХ ЗАНЯТИЙ, КОТОРОЕ ДАЁТ ИМ ОГРОМНЫЙ ПРОСТОР ДЛЯ ТВОРЧЕСТВА.** Многие занимаются этим, чтобы испытать свои навыки, другие ищут материальную выгоду. Причём далеко не всегда приходится что-то взламывать. Сколько бы ни появлялось статей о том, как важно подбирать надёжный пароль, культура интернет-безопасности в целом остаётся низкой. Пользователи интернета выбирают одни и те же незамысловатые кодовые слова для разных сайтов, переходят по подозрительным ссылкам из спама и принципиально отказываются от менеджеров паролей. Обычно злоумышленники пользуются следующими методами:

1. **ФИШИНГ.** Пользователя заманивают на сайт, который выдаёт себя за настоящий, и предлагают ввести пароль, который «утекает» к злоумышленникам;

2. **ЗЛОВРЕДНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ (MALWARE).** Такое ПО размещают на взломанных сайтах или засылают на недостаточно защищённые системы;

3. **СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ.** Иногда пароль удаётся подсмотреть, а особо доверчивые пользователи могут сообщить его злоумышленнику сами: на этом выстроен целый пласт системы интернет-мошенничества;

4. **ПОДБОР ПАРОЛЯ.** Обладая информацией о пользователе, которую легко найти в социальных сетях, можно попробовать угадать пароль. Также можно автоматом перебрать огромное количество вариантов, воспользовавшись ассоциативной базой данных или техникой словарной атаки, когда несловесные комбинации исключаются, а словесные модифицируются так, как любит большинство — заменяя буквы на похожие цифры.

Рисунок 9 — Внешний вид основных положений статьи

В статье «Безопасность в социальных сетях: не храните ключи под ковриком» [4] (рисунок 10) описываются глобальные проблемы социальных сетей с точки зрения информационной безопасности.

Многие люди, которые не знают — не застали или просто в своё время не интересовались — тёплого лампового веба эпохи 1.0, выходят в сеть исключительно ради развлечения и общения. Научно-популярные и познавательные ролики на YouTube собирают в десятки тысяч раз меньше просмотров, чем видео с танцующим енотом.

Рисунок 10 — Внешний вид скриншота сайта

В статье «Информационная безопасность» [14] (рисунок 11) в основном описывается статистика и причины взлома аккаунтов в социальных сетях.

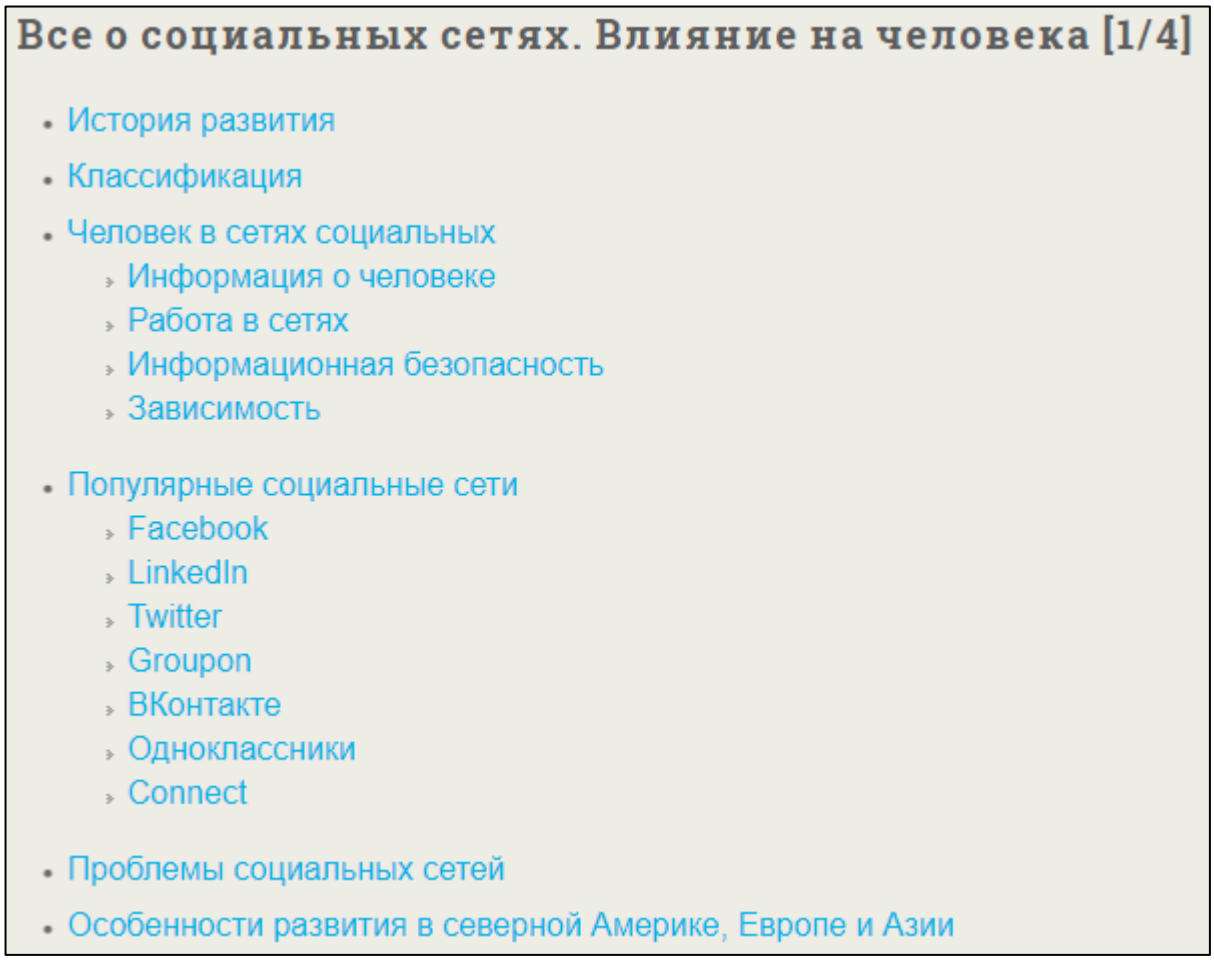
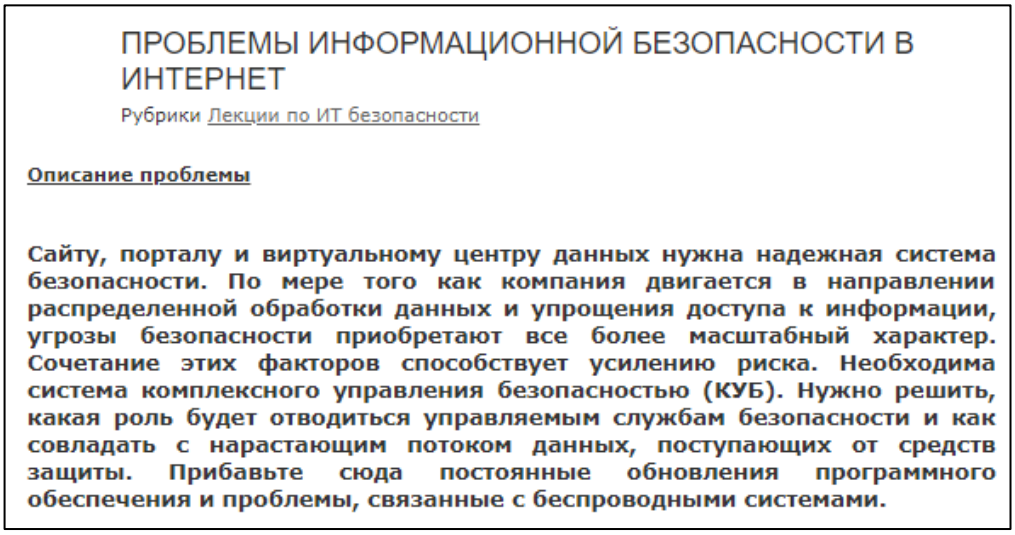



Рисунок 11 — Внешний вид оглавления сайта

В статье «Безопасность в социальных сетях.» [2] (рисунок 12) описываются основные виды социальных сетей, какие угрозы существуют, что в основном хранится на чужом аккаунте человека в социальной сети.


Рисунок 12 — Внешний вид публикации

В статье «проблемы информационной безопасности в интернете» [23] (рисунок 13) имеется много полезной информации, как с точки зрения классификации угроз информационной безопасности социальных сетей, так и методов борьбы с ними, также ко всему этому прилагается обширная статистика причин взлома аккаунтов в социальных сетях.



ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНТЕРНЕТ

Рубрики Лекции по ИТ безопасности

**Описание проблемы**

**Сайту, порталу и виртуальному центру данных нужна надежная система безопасности. По мере того как компания двигается в направлении распределенной обработки данных и упрощения доступа к информации, угрозы безопасности приобретают все более масштабный характер. Сочетание этих факторов способствует усилению риска. Необходима система комплексного управления безопасностью (КУБ). Нужно решить, какая роль будет отводиться управляемым службам безопасности и как совладать с нарастающим потоком данных, поступающих от средств защиты. Прибавьте сюда постоянные обновления программного обеспечения и проблемы, связанные с беспроводными системами.**

Рисунок 13 — Внешний вид рублики

В статье «Безопасность информации в интернете: пути решения главной проблемы мировой сети» [5] (рисунок 14) рассматриваются основные утилиты и расширения для популярных браузеров в борьбе с злоумышленниками в сети интернет, также присутствуют видео сопровождение лекции на тему «Информационная безопасность» за 2011 год.

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В ИНТЕРНЕТЕ: ПУТИ РЕШЕНИЯ ГЛАВНОЙ ПРОБЛЕМЫ МИРОВОЙ СЕТИ

*Содержание статьи:*

*Какие опасности подстерегают на просторах всемирной сети?*

*Самые распространенные проблемы и нарушения в глобальной сети*

*Использование антиспамовых блокирующих утилит*

Мировая паутина вошла в жизнь человека как один из неотъемлемых элементов быта, без которого трудно себе представить современное общество. При этом уже с момента появления данного главного распространителя информации, на первое место выступила такая идея, как информационная безопасность в интернете, поскольку она необходима и отдельным пользователям, и крупным фирмам, связывающим свою деятельность с глобальной сетью.

Рисунок 14 — Внешний вид фрагмента опубликованной лекции

В статье «Безопасный интернет детям: как защитить ребенка от негативного влияния сети?» [8] (рисунок 15) описывается что, и для чего необходимо объяснять ребенку перед тем как дать доступ в сеть Интернет.

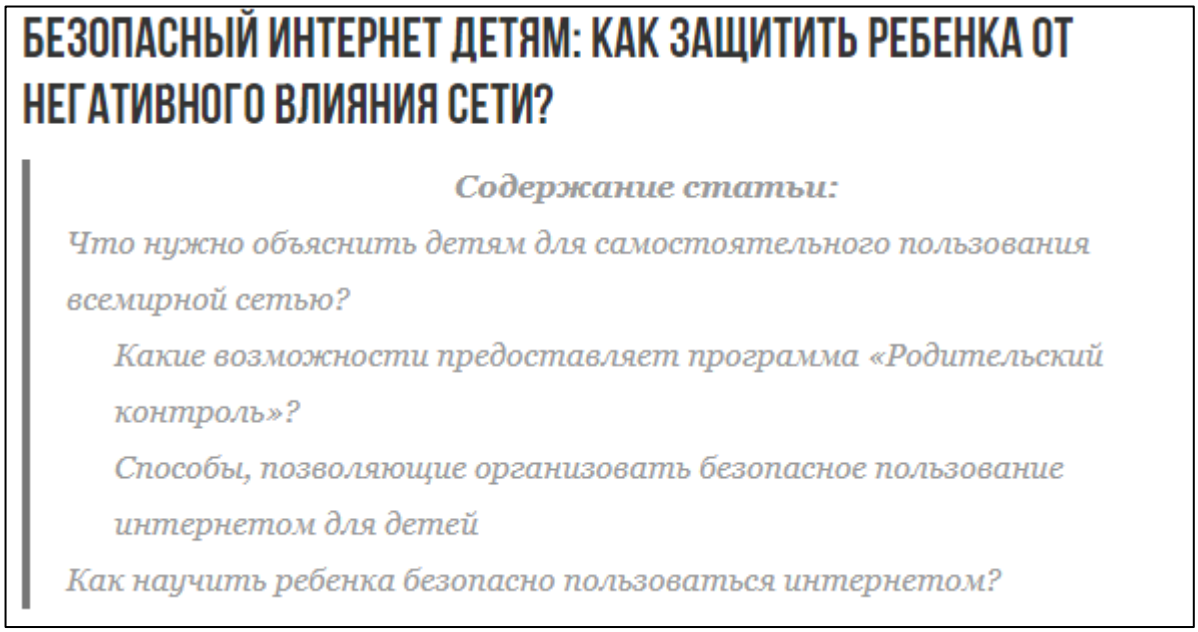



Рисунок 15 — Внешний вид оглавления статьи

В статье «Безопасность в интернете для детей обеспечивается в первую очередь родителями» [1] (рисунок 16) описывается комплекс мер для организации безопасных условий работы подростков в интернете.

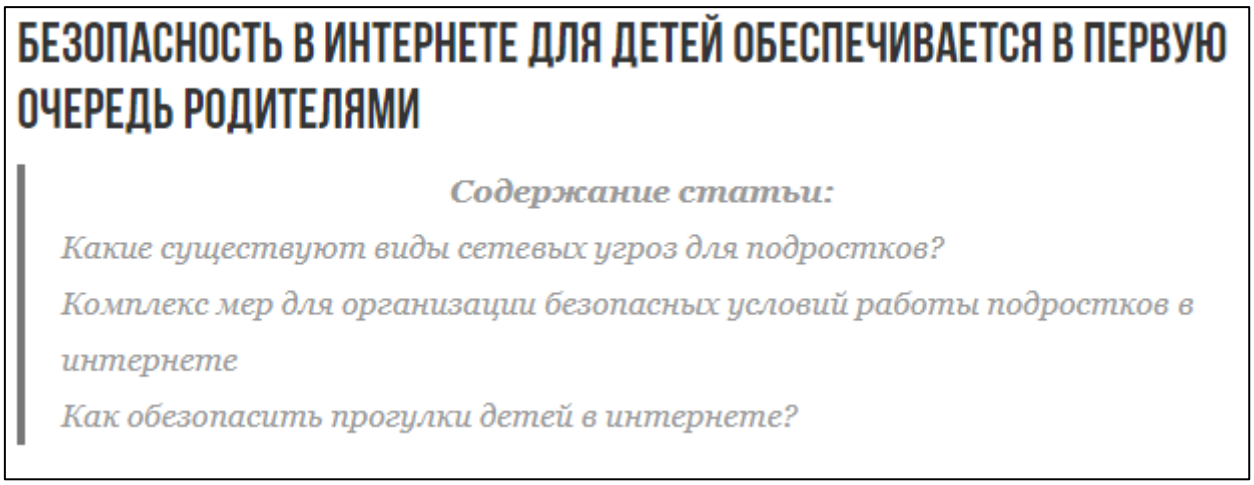



Рисунок 16 — Внешний вид основных положений статьи

В статье «Насколько безопасно хранить свою информацию в Интернете?» [20] (рисунок 17) представлен перевод статьи с иностранного языка на русский. Описывается мнение об информационной безопасности с моральной точки зрения на информационную безопасность в социальных сетях.


Рисунок 17 — Внешний вид переводного издания

В статье «Как мошенники обретают доступ к аккаунтам пользователей» [16] (рисунок 18) описывается как злоумышленник получает несанкционированный доступ к аккаунту пользователя, который ничего не подозревает, а также как уберечь доступ аккаунта от мошенников.

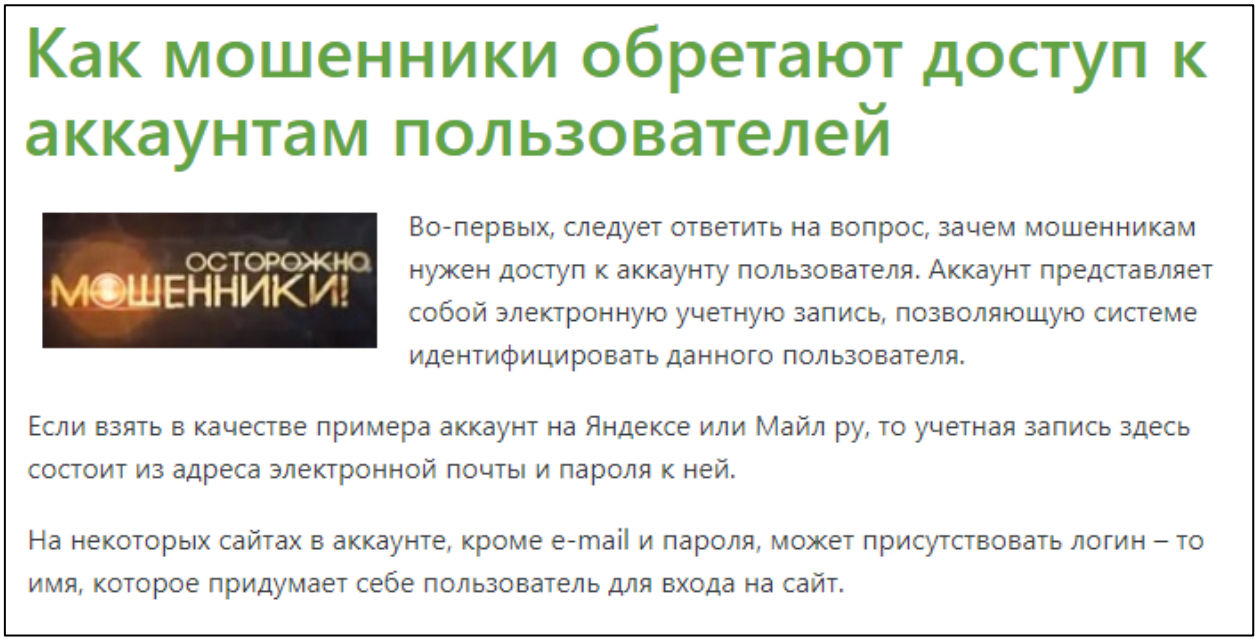



Рисунок 18 — Внешний вид скриншота сайта

В статье «Размещать это в социальных сетях опасно» [25] (рисунок 19) рассказывается как проверить свою безопасность в социальных сетях по пяти критериям, приведенным в статье.

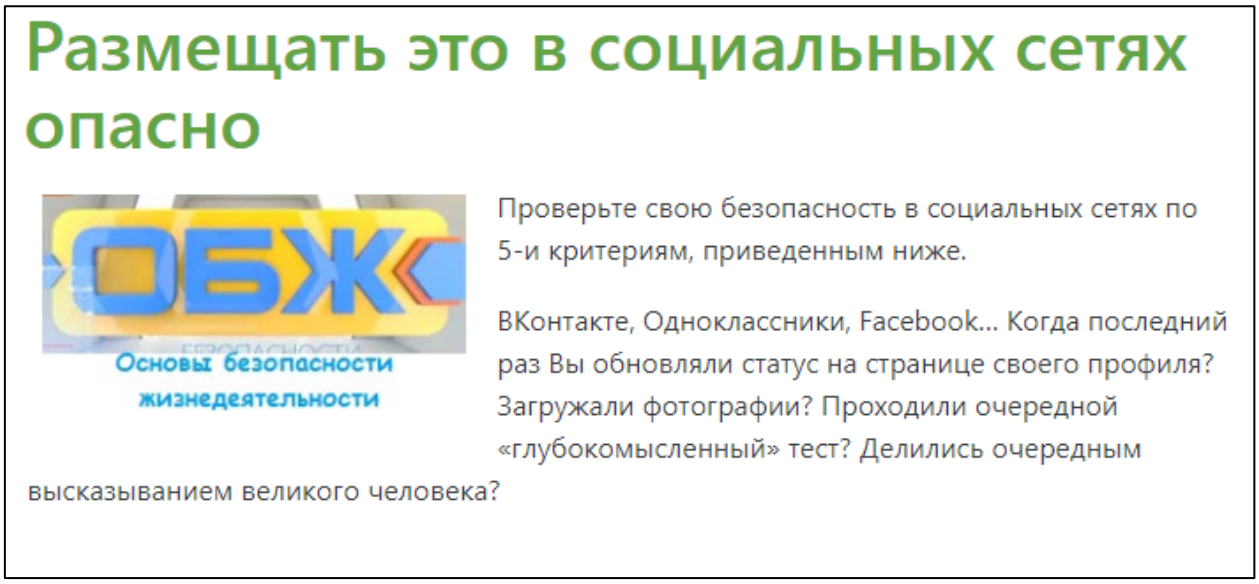



Рисунок 19 — Внешний вид статьи в разделе «Основы безопасности жизнедеятельности»

В статье (рисунок 20) «Почему люди удаляют свои аккаунты в социальных сетях?» [21] рассказывается, почему создать аккаунт в социальных сетях просто, а вот удалить что-либо очень проблематично и сложно, а иногда невозможно. Описываются различные сервисы по удалению аккаунтов социальных сетях. Как и сколько хранится ваша информация в социальных сетях, и чем это чревато.

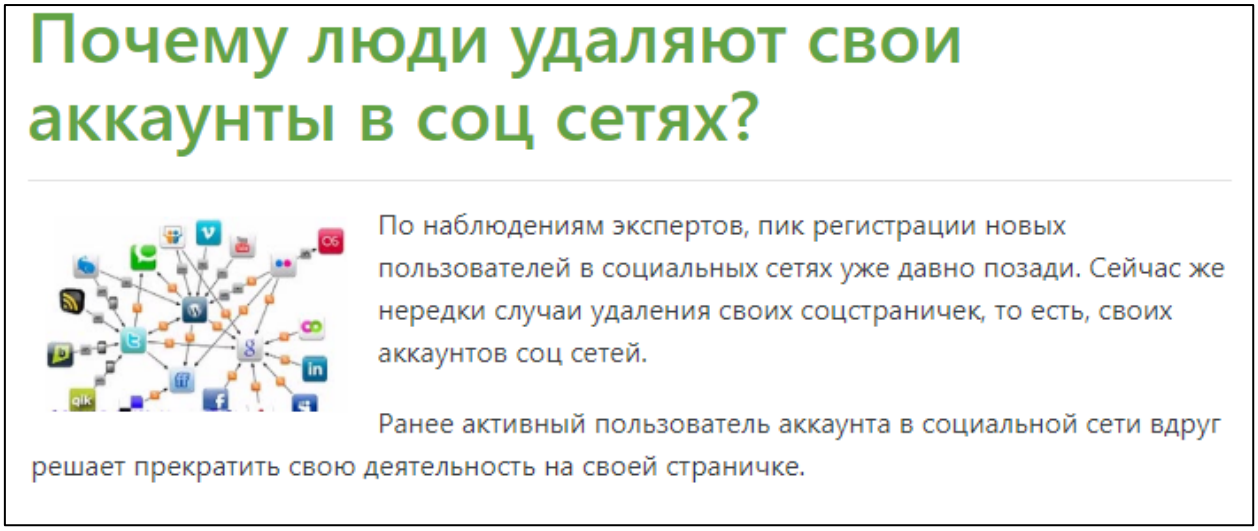



Рисунок 20 — Внешний вид интернет-статьи

В данном блоге (рисунок 21) «Безопасность в социальных сетях» [3] рассказывается о том, что необходимо задуматься о анонимизации и без-

опасности в социальных сетях, также присутствуют советы по безопасности в социальных сетях, общая настройка в социальных сетях.

Безопасность в социальных сетях

*Козлов Г.А., учитель информатики*

Согласно информации, размещенной в Википедии, социальная сеть это - платформа, онлайн сервис или веб-сайт, предназначенные для построения, отражения и организации социальных взаимоотношений. Начало бурному развитию социальных сетей положил портал Classmates.com, который оказался первой ласточкой. Позже, в 2003-2004 годах появляются такие сети как LinkedIn, MySpace и Facebook. Там же мы видим предположение, что «владельцы MySpace и Facebook сделали ставку в первую очередь на удовлетворение человеческой потребности в самовыражении. Ведь, в соответствии с пирамидой Маслоу, именно самовыражение является высшей потребностью человека, опережая даже признание и общение». Вместе с тем, социальные сети неоднородны.

Рисунок 21 — Внешний вид педагогической публикации

### 1.3 Характеристика рабочей программы

Рабочая программа по предмету «Информатика и ИКТ» для 5 — 9 классов [24] одним из вопросов содержания учебного предмета определяет тему «Работа в информационном пространстве. Информационно-коммуникационные технологии». Данная тема охватывает изучение таких вопросов, как компьютерные сети, Интернет, адресация в сети Интернет, доменная система имен, сайт, сетевое хранение данных, большие данные в природе и технике (геномные данные, результаты физических экспериментов, интернет-данные, в частности, данные социальных сетей), а также технологии их обработки и хранения.

В рамках направления «Коммуникация и социальное взаимодействие» в качестве основных планируемых результатов возможен, но не ограничивается следующим, список того, что обучающийся сможет:

- осуществлять образовательное взаимодействие в информационном пространстве образовательной организации (получение и выполнение заданий, получение комментариев, совершенствование своей работы, формирование портфолио);
- использовать возможности электронной почты, интернет-мессенджеров и социальных сетей для обучения;

- вести личный дневник (блог) с использованием возможностей сети Интернет;
- соблюдать нормы информационной культуры, этики и права; с уважением относиться к частной информации и информационным правам других людей;
- осуществлять защиту от троянских вирусов, фишинговых атак, информации от компьютерных вирусов с помощью антивирусных программ;
- соблюдать правила безопасного поведения в сети Интернет;
- различать безопасные ресурсы сети Интернет и ресурсы, содержание которых несовместимо с задачами воспитания и образования или нежелательно.

### 1.4 Общие требования к пользовательскому интерфейсу

Основным требованиями к структуре комплекса электронных материалов, является представление информации пользователю в удобном, простом, и понятном интерфейсе, а также обязательное наличие иллюстраций в высоком качестве.

Требования функционального характера:

- обеспечение корректной навигации, наличие теоретического материала, наличие ознакомительных видео, качественный интерфейс, качественная интеграция контента в структуру комплекса электронных материалов.
- обеспечить корректное отображение элементов продукта, а также предоставить оптимизированную версию продукта для мобильных устройств.

В связи с тем, что, строгая стандартизация оформления интерфейсов сайта отсутствует, но они все-таки есть.

Было принято решение использовать следующие принципы:

- принцип пропорции, для данного принципы необходимо соблюдать простые правила, для того что бы информация не была хаотично расположена на экране;
- принцип равновесия, равномерное расположение оптической тяжести на экране;
- принцип единства, все изображения должны быть взаимосвязаны, то есть правильное соотношение размеров, форм, цветовой схемы.

Идентичные данные обязательно должны быть представлены однотипно, с использованием рамок и полей.

Цветовая схема не должна быть слишком вызывающей, сливающейся с фоном информации, никаких ярких вызывающих дискомфорт цветов.

# 2 ОПИСАНИЕ КОМПЛЕКСА ЭЛЕКТРОННЫХ МАТЕРИАЛОВ

## 2.1 Описание структуры

После проведенной работы была разработана структура (рисунок 22) комплекса электронных материалов по информационной безопасности в социальных сетях которая состоит из:

1. Графический интерфейс программы.
2. Введение.
3. Теоретический материал, описывающий, и раскрывающий различные проблемы.
4. Видеоматериалы, раскрывающие проблему.
5. Об авторе.
6. Список используемых источников.

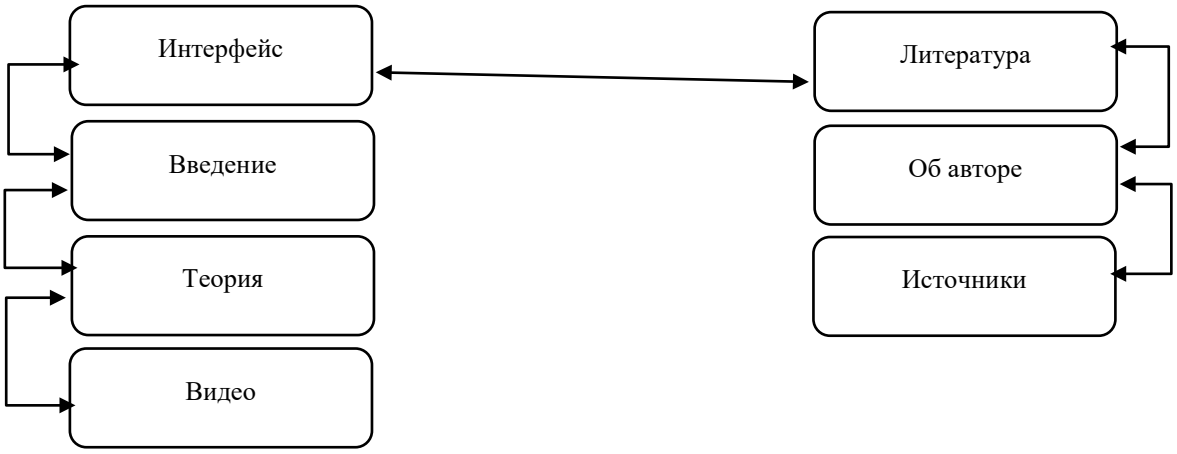



Рисунок 22 — Структура комплекса электронных материалов

## 2.2 Описание интерфейса комплекса электронных материалов

Главная страница (рисунок 23) содержит краткую актуальность темы, а также навигационные кнопки, для подробного ознакомления с полной информацией.

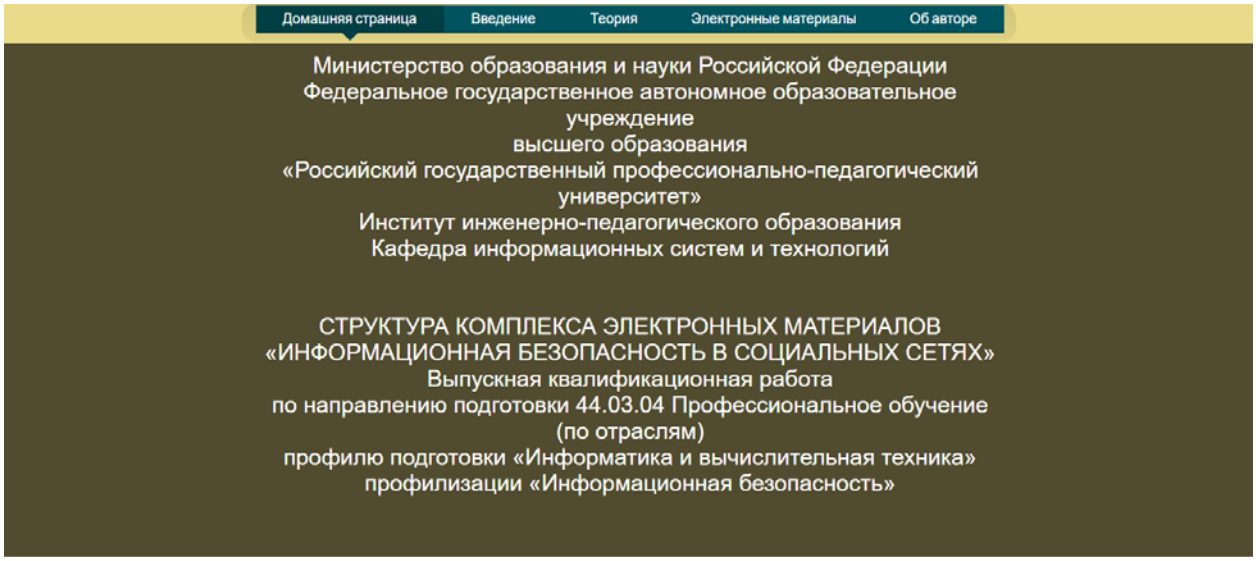



Рисунок 23 — Домашняя страница

На рисунке изображен снимок экрана (рисунок 24) раздела «Введение».

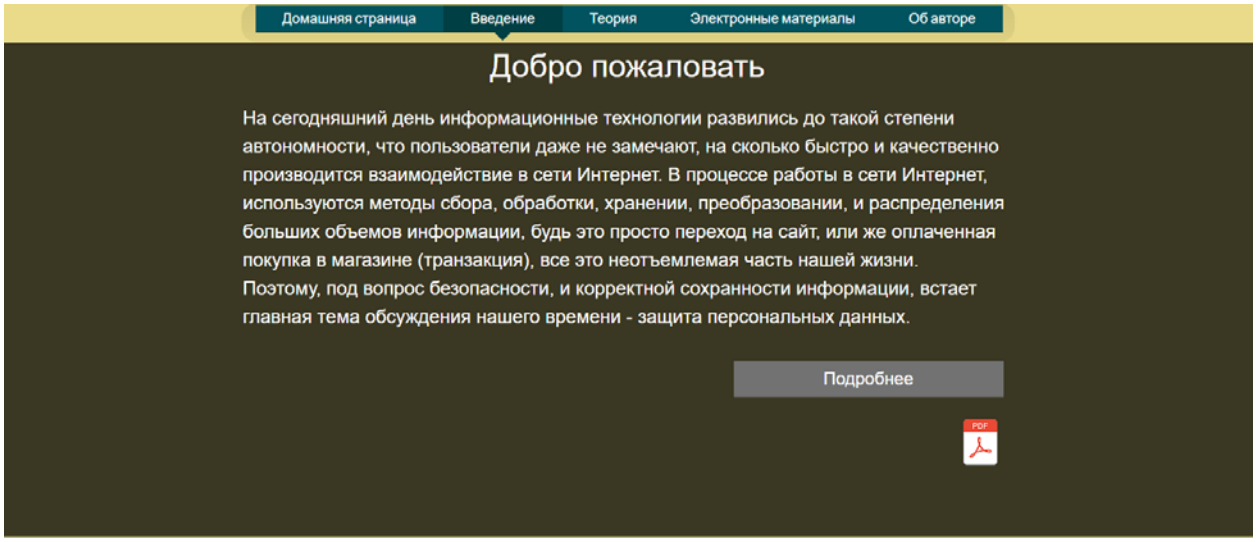



Рисунок 24 — Внешний вид раздела «Введение»

На изображении (рисунок 25) показан результат перехода по навигационной кнопке «Подробнее».

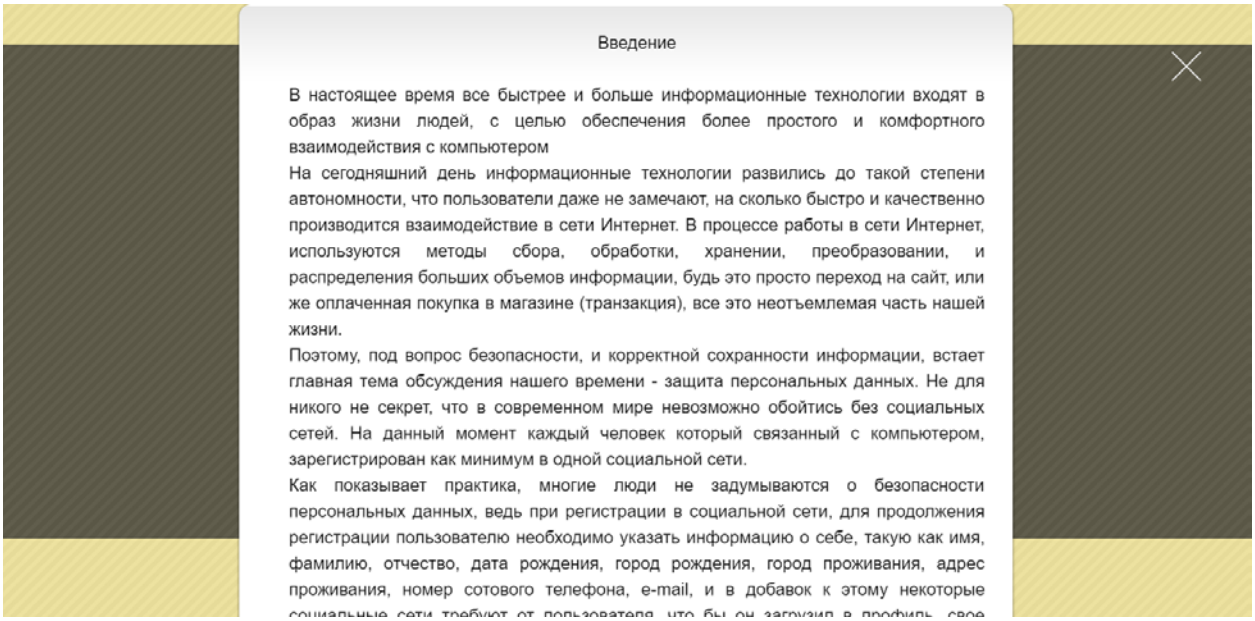



Рисунок 25 — Результат действия навигационной кнопки

На рисунке изображен подраздел «Теория» (рисунок 26) на тему «что такое социальные сети?».

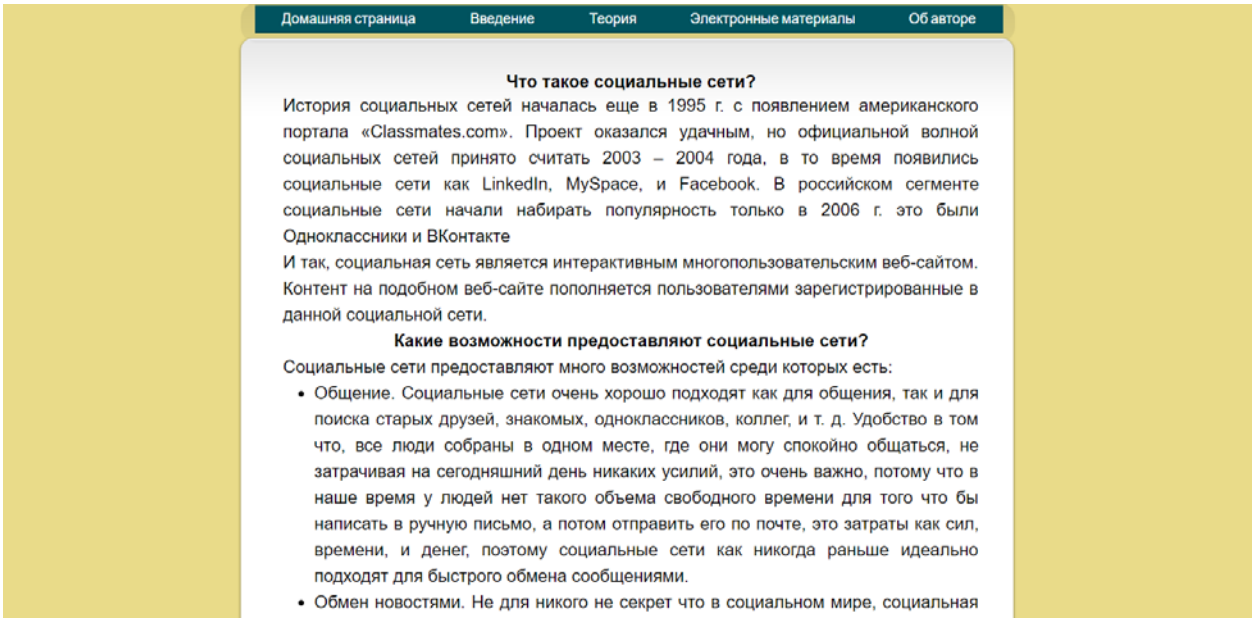



Рисунок 26 — Внешний вид подраздела «Теория»

На рисунке демонстрируется раздел «Электронные материалы», содержащий меню в виде плиток, которое обеспечивает навигацию по видеоматериалам (рисунок 27).


Рисунок 27 — Внешний вид раздела «Электронные материалы»

На рисунке изображен один из подразделов (рисунок 28) «Электронные материалы», содержащий видеоматериал, размещенный на хостинге «YouTube».

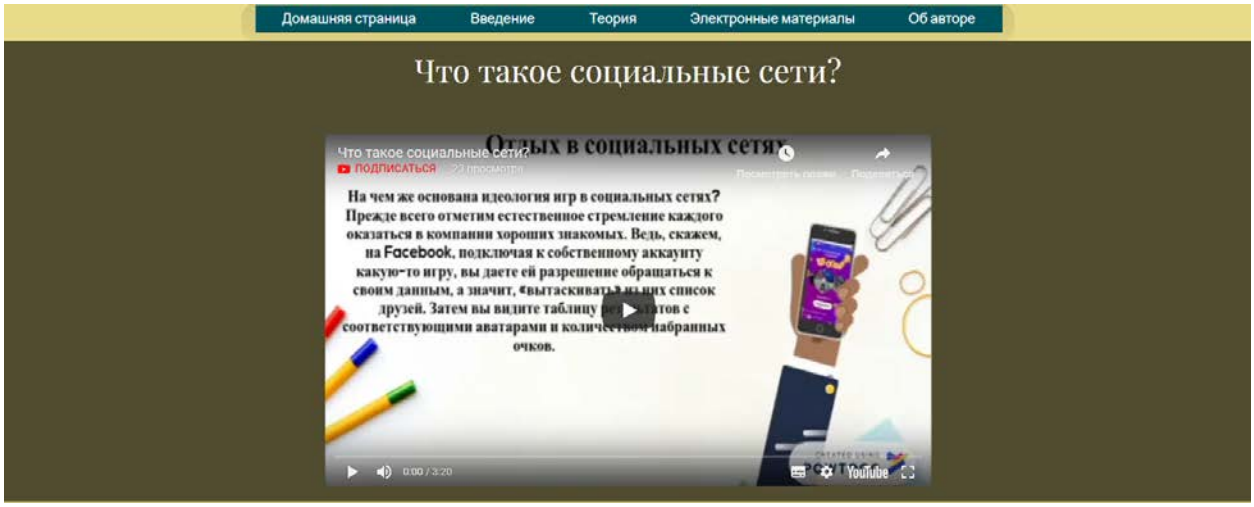



Рисунок 28 — Внешний вид подраздела «Электронные материалы»

На рисунке изображен раздел об авторе (рисунок 29), содержит информацию об авторе, а также обратная связь с ним.

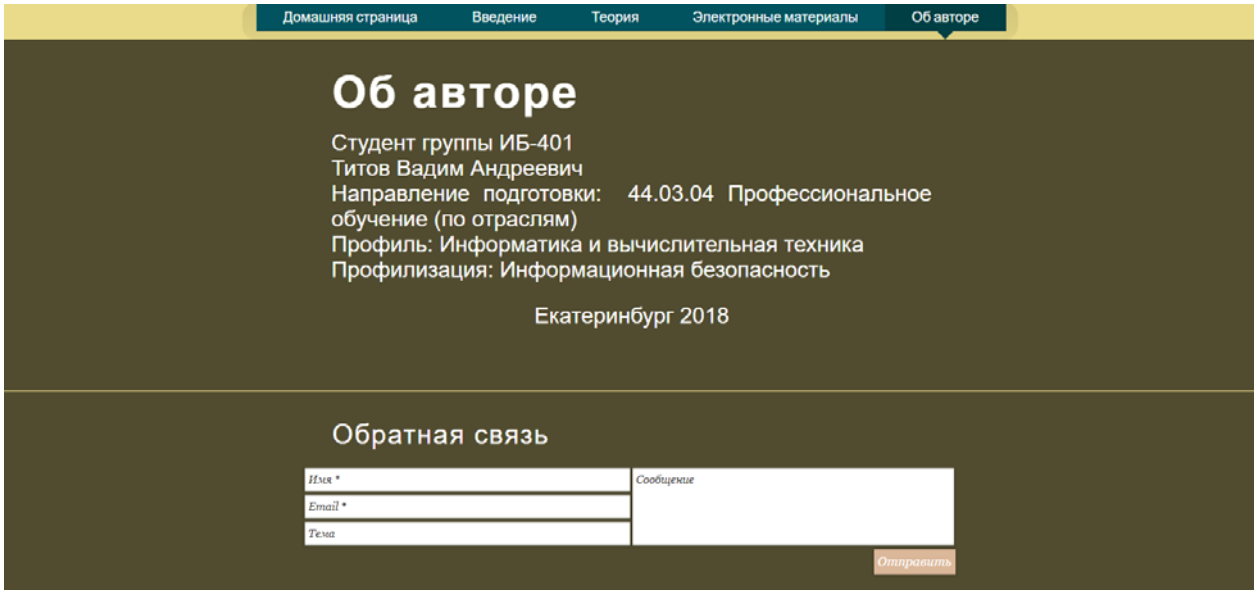



Рисунок 29 — Внешний вид раздела «Об авторе»

## 2.3 Описание интерфейса мобильной версии комплекса электронного материала

Процент людей, которые пользуются Интернетом с помощью смартфонов и планшетов, продолжает расти. Это связано, в первую очередь, с удобством и ростом скорости доступа.

Вот только далеко не все веб-сайты нормально отображаются на экранах мобильных устройств, поскольку изначально были сделаны с ориентацией на стандартное разрешение стационарных мониторов.

Это создает ряд проблем при навигации пользователя, что часто приводит к тому, что человека это раздражает, и он просто покидает ресурс. Поэтому, стоит рассмотреть возможность адаптации сайтов под мобильные устройства.

Благодаря широким возможностям редактора сайтов, было принято решение оптимизировать основную версию сайта, под планшетные и мобильные устройства.

На изображении (рисунок 30) показана мобильная версия домашней страницы сайта.

Данная версия сайта позволяет без проблем пользоваться сайтом, благодаря мобильной оптимизации.

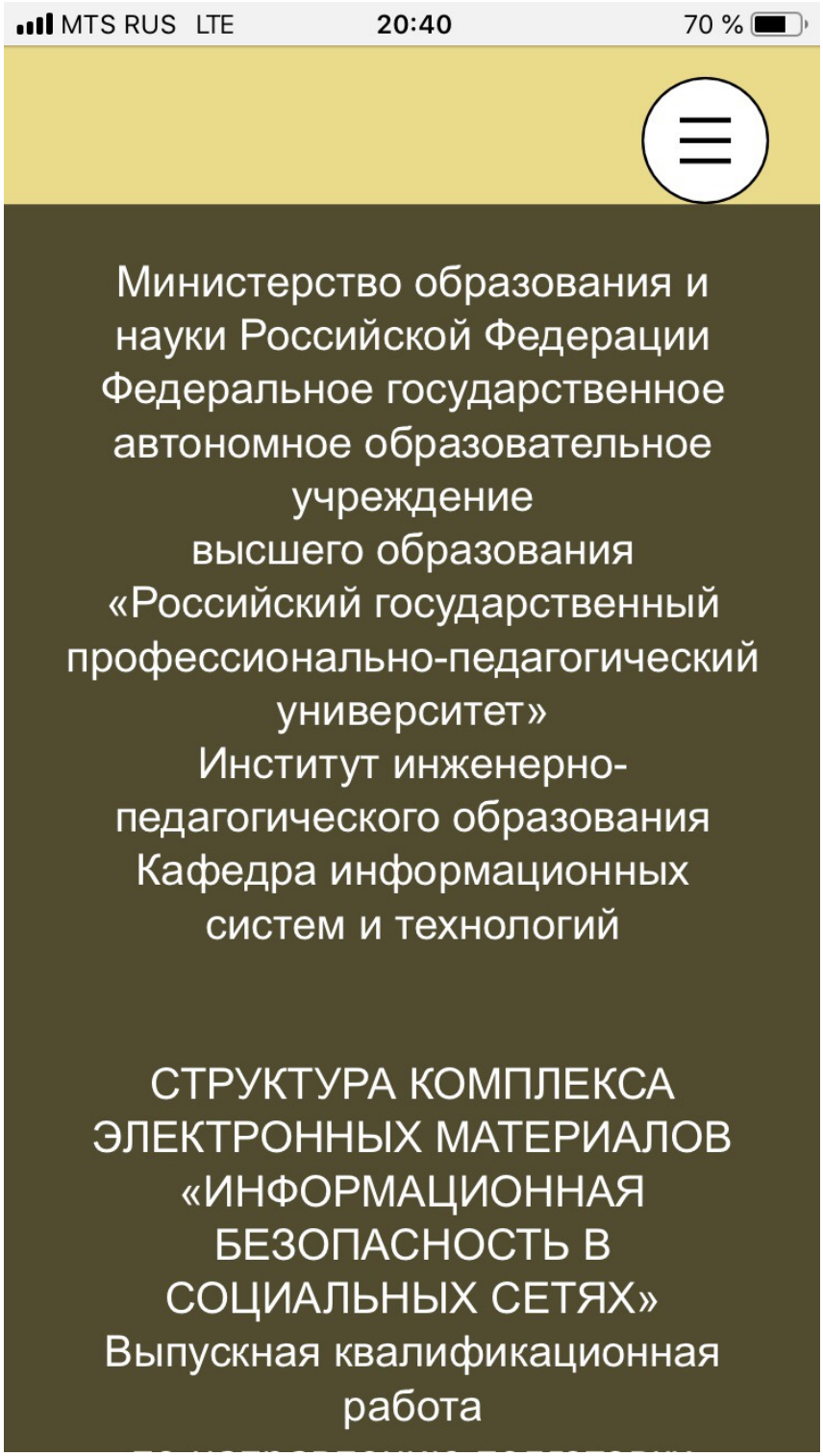



Рисунок 30 — Внешний вид главной страницы мобильной версии

На изображении (рисунок 31) показана работа навигационной кнопки в мобильной версии сайта, навигационная кнопка меню находится в шапке сайта. Мобильная версия сайта позволяет пользователям, использовать сайт с

теми же функциями что и на основной версии сайта, только в более удобном варианте.

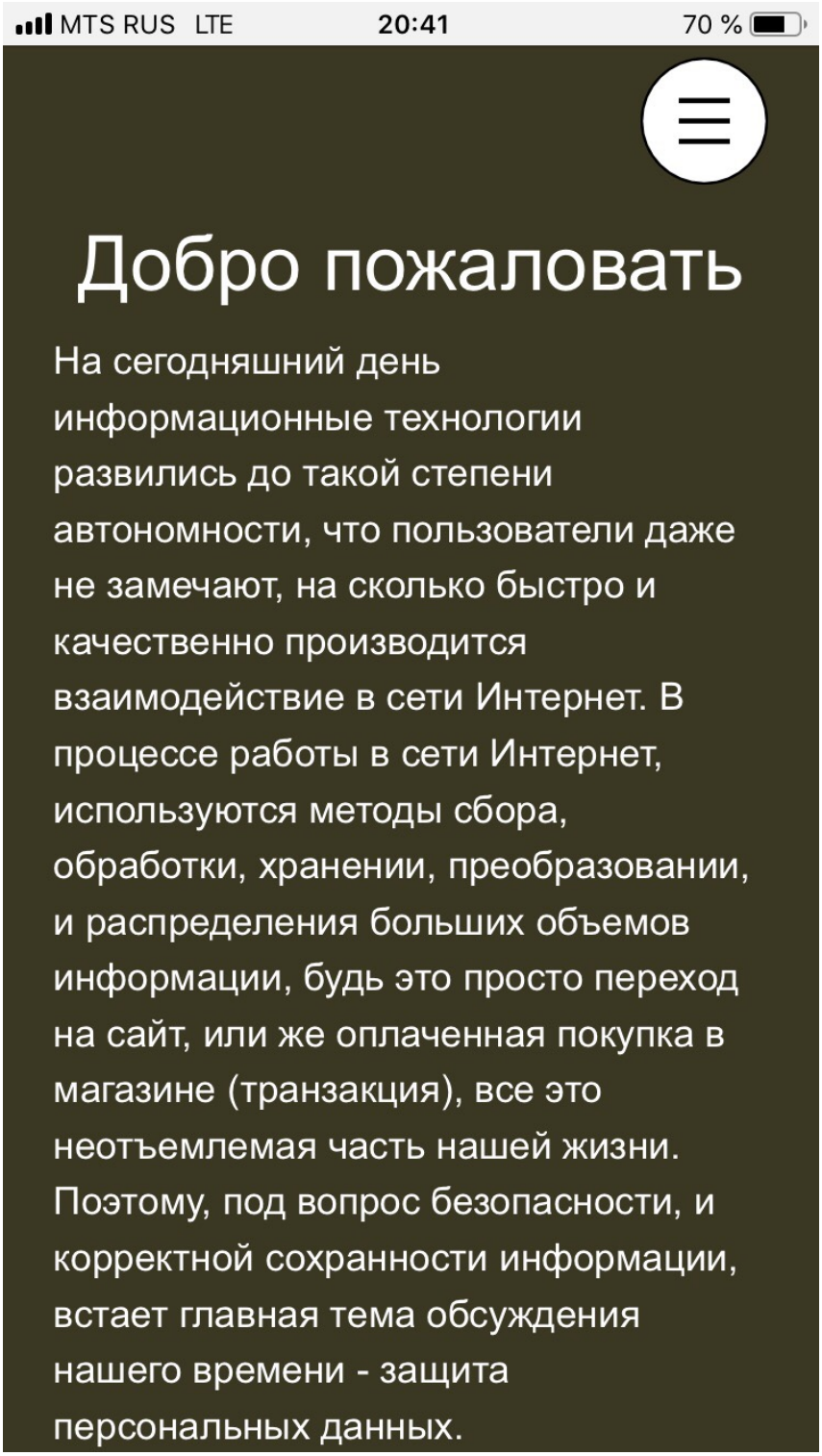



Рисунок 31 — Внешний вид раздела «Введение» мобильной версии

На изображении (рисунок 32) показана мобильная версия одного из раздела литературы, на примере темы «Что такое социальные сети?». Навигационная кнопка возврата в раздел ваше, находится с низу, однако пользо-

ватель может обратиться в навигационное меню, располагающаяся в шапке сайта.


Рисунок 32 — Внешний вид раздела «Литература» мобильной версии

На изображении (рисунок 33) показана мобильная версия раздела электронные материалы. В данном разделе присутствует меню в виде плиток,

благодаря этому выбор одной из тем осуществляется нажатием одной из плиток.

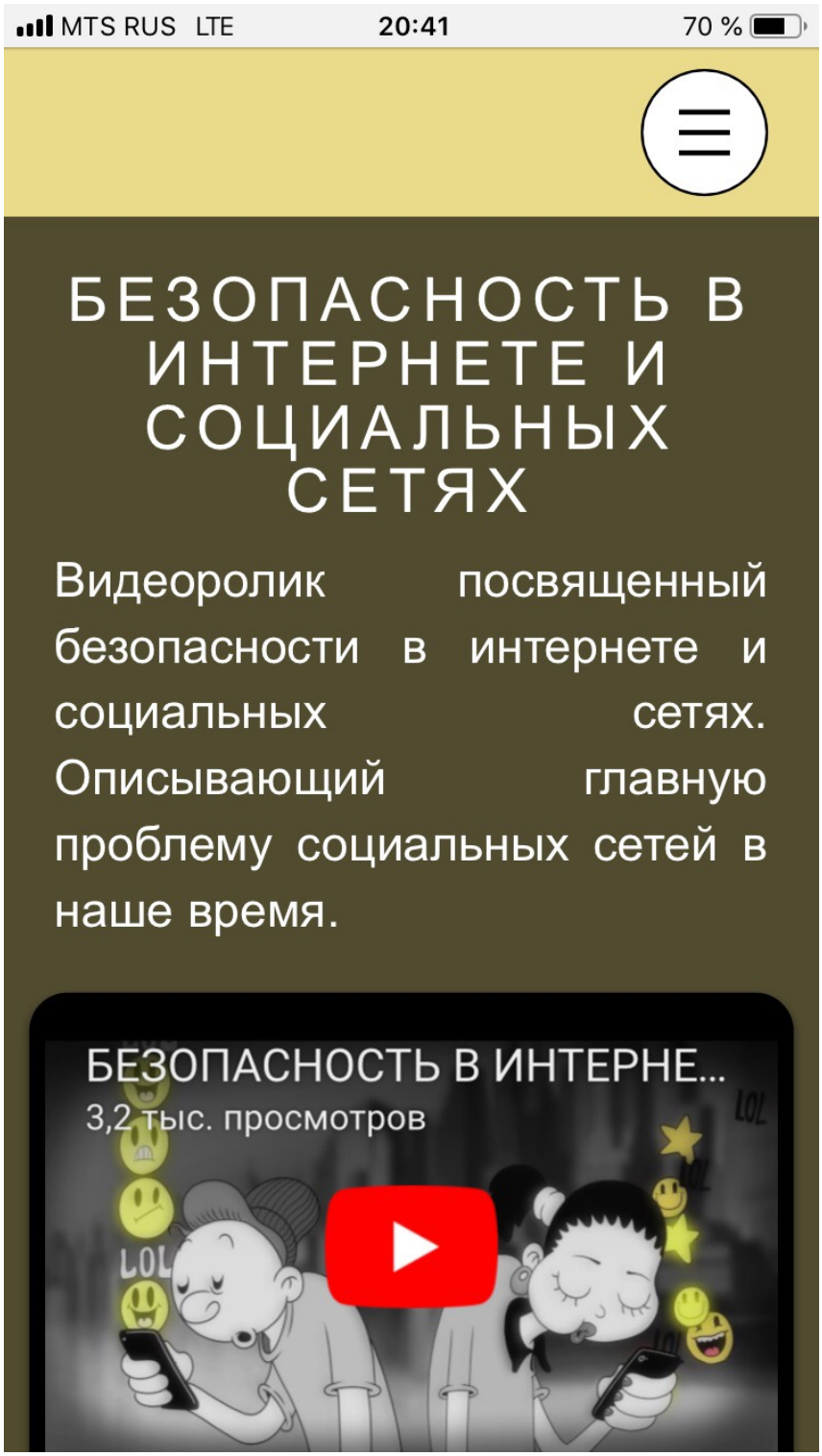



Рисунок 32 — Внешний вид раздела «Электронные материалы» мобильной версии

На изображении (рисунок 34) показана мобильная версия подраздела электронных материалов, на примере «Что такое социальные сети». Выход в

предыдущее меню осуществляется навигационной кнопкой «Меню», находящаяся в шапке сайта.

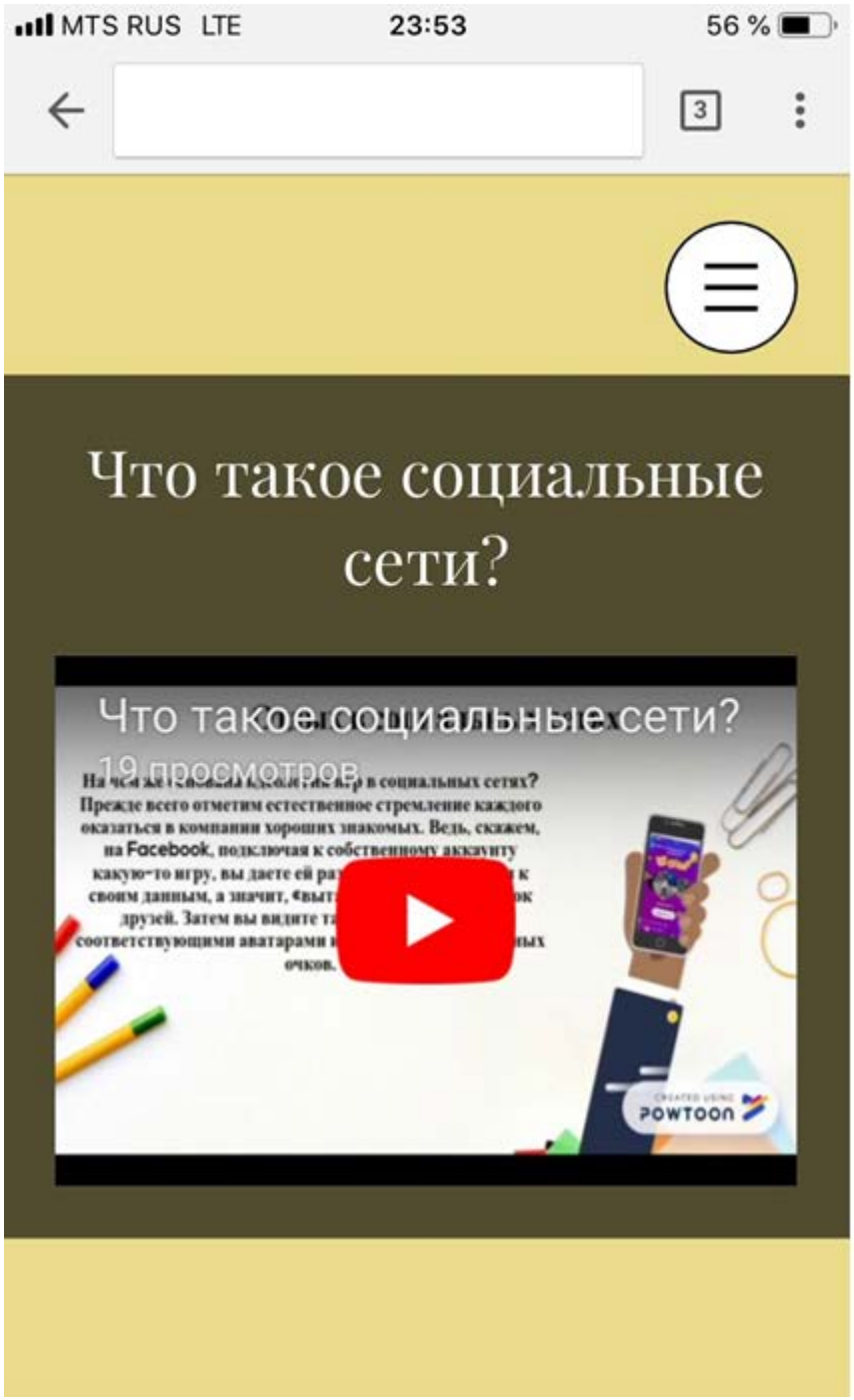



Рисунок 34 — Внешний вид подраздела «Электронные материалы» мобильной версии

На изображении (рисунок 35) показана мобильная версия раздела «Об авторе». Выход в предыдущее меню осуществляется навигационной кнопкой «Меню», находящаяся в шапке сайта.

Также в данном разделе располагается форма обратной связи.

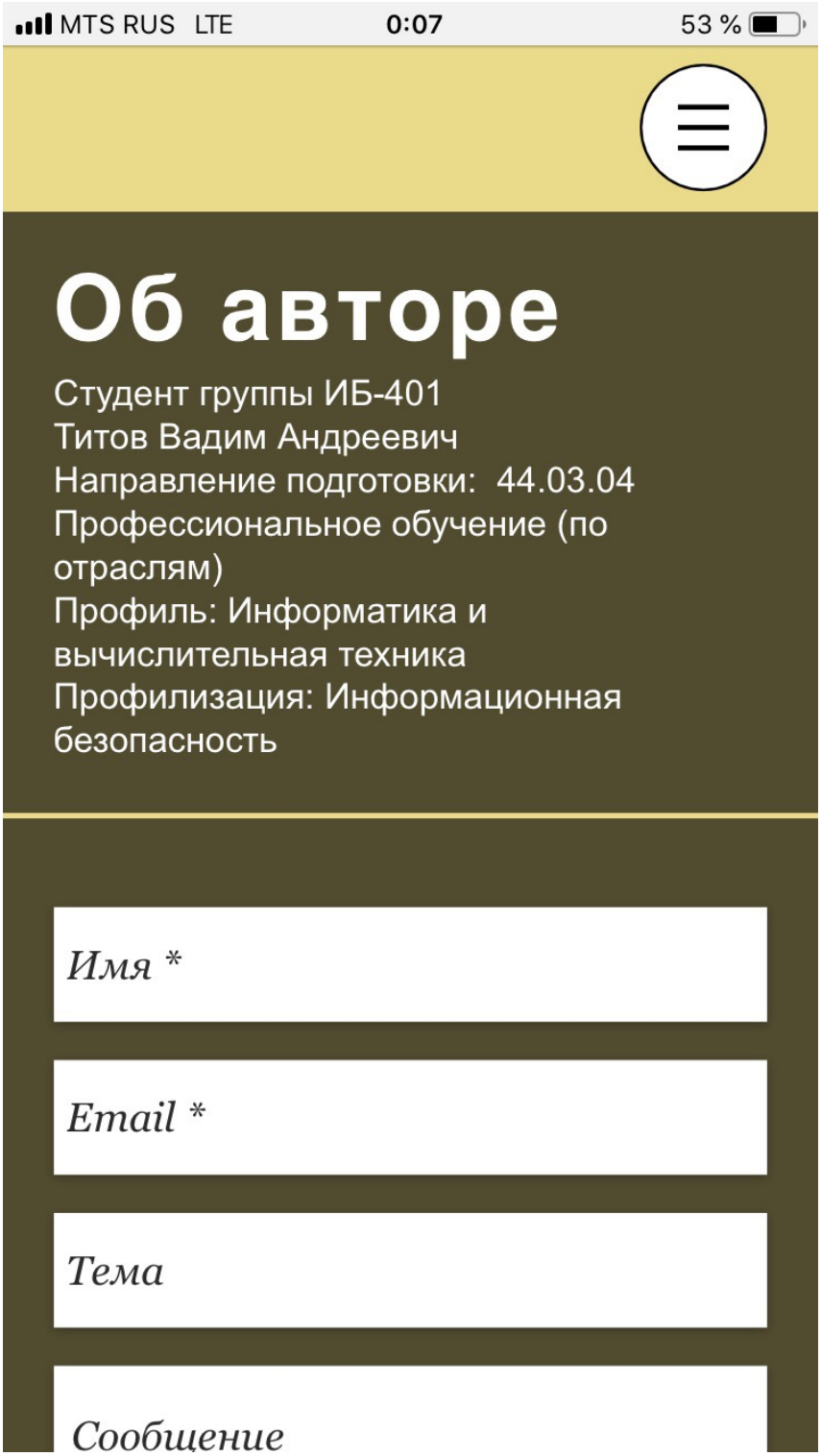



Рисунок 35 — Внешний вид раздела «Об авторе» мобильной версии

## 2.4 Описание тематики комплекса электронных материалов

Комплекс электронных материалов содержит образовательную тематику, направленную на теоретическую осведомленность, обеспечивающее пра-

вильность настройки параметров приватности в социальных сетях с целью обеспечения информационной безопасности, а также конфиденциальности персональных данных пользователей.

В современном мире, не что так не ценится как — информация. Поэтому в комплексе электронных материалов рассматриваются такие проблемы как:

- халатность пользователей в отношении персональных данных;
- не внимательность во время настройки параметров конфиденциальности информации отображаемая в социальных сетях;
- причины взлома аккаунтов в социальных сетях;
- вредоносное ссылки, приложения в социальных сетях.

До появления цифровой эры — люди умели хранить свои секреты, в наше же время оставить что-то конфиденциальное в сети Интернет приближается к невозможности.

Защита персональных данных — это важная проблема в наше время для людей всех возрастов. Дело в том, что ваши данные все данные хранятся на различных серверах в сети Интернет, поэтому становится страшно от мыслей, что, когда вы набираете сообщение, или загружаете фото, не вольно задумываетесь о том, что, а вдруг это попадет не в те руки. Никто не застрахован от сбоя в программе, также, как и от человеческого фактора что в практике встречается чаще.

Также в комплексе электронных материалов раскрываются такие темы как:

- с какой целью и для чего взламывают аккаунты пользователей;
- ошибки пользователей в сети интернет, которые влияют на безопасность аккаунта в социальных сетях;
- как защитить свой аккаунт в социальных сетях;
- правила поведения в социальных сетях.

Социальные сети на сегодняшний день — неотъемлемая часть современной жизни. Поэтому перед тем как заполнять свой профиль в социальной

сети стоит задуматься о том, что социальная сеть — это большая база данных не только общедоступной информации, но и информации пользователей. Личная информация в основном доступна определенному кругу лиц, например, находящихся в списке друзей. Однако если аккаунт будет взломан, то вся конфиденциальная информация будет доступна всей сети, в том числе и злоумышленникам, и будет использована в корыстных целях. В одном из разделов будет описание, для чего взламывают аккаунты; по чьей вине безопасность аккаунтов в социальных сетях страдает от злоумышленников, а также какие последствия могут быть с пользователем, у которого взломали аккаунт в социальной сети. Также в одном из разделов будут рассмотрены способы защиты своих персональных данных.

### 2.5 Преимущества использования видеоматериалов

За последние годы информационные технологии сильно повлияли на жизнь общества в целом. Без них в наше время трудно представить современного человека, потому как информационные технологии все шире используются в образовательном процессе, например, видеоматериалы.

На сегодняшний день видеоматериалы все больше используются в образовательном процессе. Главным преимуществом этой технологии является наглядное представление, что очень важно для того чтобы демонстрационный материал усваивался благоприятно, так как большая часть усваивается зрительной памятью, и создаются ассоциативные понятия. Видеоматериалы не чуть не хуже, чем урок с классифицированным преподавателем, их эффективность вполне сравнится с дорогостоящими курсами в учебных центрах. Также видеоматериалы позволяют усваивать материал гораздо быстрее, чем любая книга, для того что бы начать пользоваться данной технологией, можно воспользоваться материалами интернета. Видеоматериалы бывают разными, и их количество растет с каждым днем, существуют разные тематики видеоматериалов, например, от приготовления вкусной еды, до детального рас-

смотрения боевых приемов. Но самое большое количество занимают видеоматериалы посвященных материалам на учебную тематику.

Плюсы видеоматериалов:

- доступность. сейчас абсолютно не трудно отыскать в интернете интересующий материал, включить видеоматериал и начать изучать его. нужен только какое-нибудь устройство (компьютер, планшет, смартфон), стабильное соединение с интернетом и желание. таким образом, любой желающим в свободное от основного занятия время может подучиться чему-то новому.

- экономия. При изучении видеоматериала не нужно трать собственное время на то, чтобы добраться до школы, института, тренингового цента или другого учебного заведения. Необходимо все лишь найти интересующий материал и приступать к ознакомлению. Также нет нужды платить за обучение. В сети есть достаточно доступной информации. Конечно, стоит учесть, что лучшие видеокурсы и онлайн-программы обучения, составленные профессиональными преподавателями, являются платными, и в некоторых случаях без оплаты не обойтись. Но в любом случае это будет дешевле, чем ехать жить на несколько месяцев или лет в другой город или даже страну, чтобы получить желаемые знания.

- психологический фактор. Каждый человек индивидуален. Кто-то любит находиться в центре внимания, выступать на публики и быть в больших аудиториях. А для кого-то намного комфортнее сидеть в своем доме, в привычной обстановке и не отвлекаться на других людей. Для таких студентов учеба по видеоматериалам является идеальной формой получения знаний.

- свободный график. Для многих людей обучение является невозможным из-за работы и других дел. Особенно это касается рабочих, которые находятся на каких-либо должностях и хотели бы повысить квалификацию или выучиться на другую профессию, но жесткий график не позволяет им этого сделать. В таком случае видеоматериалы станут единственным решением. Человек сможет обучаться дистанционно в любое удобное время.

## 2.6 Описание созданных видеоматериалов

Для комплекса электронных материалов, были созданы видеоматериалы, они размещены в разделе «Электронные материалы». Каждый видеоматериал имеет приятную анимацию, благодаря различным интернет ресурсам были созданы видеоматериалы с использованием анимаций, что добавляет принцип наглядности. Каждый видеоматериал имеет теоретический материал, который описывает главную проблему, пути их решения, примеры, и описание, для подробного изучения темы, пользователю предполагается перейти в раздел «Теория», для дальнейшего глубокого ознакомления с темой видеоматериала. Каждый видеоматериал имеет текстовую версию темы, и является дополнением, для самостоятельного изучения. Все видеоматериалы по времени рассчитаны на небольшие темы, и составляют примерно от 5 минут до 10, сделано это в первую очередь для того что бы сократить зрительную нагрузку на пользователя, просматривающего данные видеоматериалы. Каждый видеоматериал был создан с использованием озвучивания, то есть каждый ролик имеет озвучку с последующими пояснениями и комментариями. Плюсы данных видеоматериалов являются:

- экономия времени;
- небольшой объем информации;
- минимальное по времени зрительная нагрузка;
- возможность неоднократного просмотра;
- доступ с любого устройства;
- поддержка смартфонов, планшетов;
- доступ из любой точки мира, в любое время;
- озвучка видеоматериалов.

Видеоматериал считается одним из самых быстрых и легких способов обучения. Учащиеся имеют возможность одновременно читать, просматривать изображения и графики, воспринимать на слух и смотреть видео.

Еще одно преимущество — индивидуальность обучения. Это дает возможность хорошо усвоить урок. Например, если какой-то момент непонятный, то его можно сразу включить повторно, пока не будет все усвоено правильно. Также существует обратная связь с автором, если что-то не понятно, можно написать на почту автору. Причем одно и то же место в видеоматериале можно включать бесконечное количество раз. И самое главное, что может быть важно для любого человека — это возможность сэкономить деньги на обучении.

# ЗАКЛЮЧЕНИЕ

В заключении хотелось бы сказать о том, что все поставленные в выпускной квалификационной работе задачи были решены в полном объеме. Цель достигнута.

В процессе работы над выпускной квалификационной работой были решены следующие задачи

- была изучена литература по информационной безопасности в социальных сетях, с целью определения проблем безопасности детей при их общении в любой из социальных сетей;
- были определены критерии и требования к структуре комплекса электронных материалов «Информационная безопасность в социальных сетях»;
- был реализован комплекс электронных материалов «Информационная безопасность в социальных сетях».

Вывод такой — интернет общение должно дополнять окружающий мир, а не становиться одной из зависимостей современного мира. Стоит задуматься о том какую конфиденциальную информацию вы размещаете в той или иной сети. Не стоит забывать о том, что существуют настройки приватности для отображения в отношении других пользователей информации в социальной сети. Необходимо отдавать себе отчетность в том, что не надо вести важную конфиденциальную переписку в социальных сетях, этого можно избежать, договорившись о личной встрече, скорее всего это отнимет у вас какое-то время, но вы будете спокойнее с точки зрения того, что вашу информацию не прочтет кто-либо другой, в том числе и мошенник.

Конечно, проблема не столько в пользователях, сколько в отсутствии некого единого свода правил поведения в сети. Детям с малых лет объясняют, почему нельзя переходить дорогу на красный свет светофора — уже давно имеет смысл с малых лет учить составлять и безопасно хранить свои па-

роли, не оставлять их где попало и критически оценивать просьбы незнакомцев поделиться личной информацией.

Также, эта тема касается тех фото, которые вы загружаете в социальные сети будь то это открытый доступ или личная переписка, не стоит загружать фото своих кредитных и банковских картах. И именно сейчас есть чудесная возможность воспитать в подрастающем поколении уважение к собственным приватным данным почти с пелёнок. Это дело учителей, преподавателей, родителей. Знания о правилах безопасного поведения в интернете уже давно вышли за рамки дополнительной информации, которую можно либо принять во внимание, либо забыть. Однако до сих пор большинство пользователей халатно относятся к своим персональным данным, находясь в состоянии заблуждения, что их информация некому не нужна.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ


1. Безопасность в интернете для детей обеспечивается в первую очередь родителями [Электронный ресурс] — Режим доступа — https://camafon.ru/internet/bezopasnost-detey (дата обращения: 02.04.2018).

2. Безопасность в социальных сетях [Электронный ресурс] — Режим доступа — https://whoer.net/blog/bezopasnost-v-socialnyx-setyax/ (дата обращения: 02.04.2018).

3. Безопасность в социальных сетях [Электронный ресурс] — Режим доступа — http://www.1060.ru/bezopasnost_v_socialnykh_setjakh/ (дата обращения: 02.04.2018).

4. Безопасность в социальных сетях: не храните ключи под ковриком [Электронный ресурс] — Режим доступа — https://newtonew.com/tech/social-engineering-in-social-networks (дата обращения: 02.04.2018).

5. Безопасность информации в интернете: пути решения главной проблемы мировой сети [Электронный ресурс] — Режим доступа — https://camafon.ru/internet/informatsionnaya-bezopasnost (дата обращения: 02.04.2018).

6. Безопасность персональных данных в социальных сетях [Электронный ресурс] — Режим доступа — http://human.snauka.ru/2015/11/13018 (дата обращения 02.04.2018).

7. Безопасность персональных данных в социальных сетях [Электронный ресурс] — Режим доступа — http://www.itsec.ru/articles2/pravo/zaschi-ta-personalnyh-dannyh-v-sotsialnyh-setyah (дата обращения: 02.04.2018).

8. Безопасный интернет детям: как защитить ребенка от негативного влияния сети? [Электронный ресурс] — Режим доступа — https://camafon.ru/internet/bezopasnyiy (дата обращения: 02.04.2018).

9. Виды рисков для пользователей социальных сетей [Электронный ресурс] — Режим доступа — http://www.mce.su/rus/archive/abstracts/mce19/sect128328/doc150831/ (дата обращения 06.04.2018)

10. Влияние социальных сетей на психику личности [Электронный ресурс] — Режим доступа — http://rostduha.ru/vlieanie-socialinih_setei/ (дата обращения 06.04.2018).

11. Виды защиты информации в социальных сетях [Электронный ресурс] — Режим доступа — https://sites.google.com/site/socialnyeseti94/zasita-informacii-v-socialnyh-setah/vidy-zasity-informacii-v-socialnyh-setah (дата обращения 06.04.2018).

12. Защита персональных данных в социальных сетях [Электронный ресурс] — Режим доступа — https://www.osp.ru/cio/2011/12/13012286/ (дата обращения: 02.04.2018).

13. Защита персональных данных в социальных сетях [Электронный ресурс] — Режим доступа — http://www.itsec.ru/articles2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah-ib-5-2016/ (дата обращения: 02.04.2018).

14. Информационная безопасность [Электронный ресурс] — Режим доступа — https://secl.com.ua/article-vse-o-socialnyh-setjah-vlijanije-na-cheloveka.html#part33 (дата обращения: 02.04.2018).

15. Как именно хакеры взламывают аккаунты в социальных сетях [Электронный ресурс] — Режим доступа — http://www.lookatme.ru/mag/how-to/security/206725-hacking-accounts (дата обращения: 02.04.2018).

16. Как мошенники обретают доступ к аккаунтам пользователей [Электронный ресурс] — Режим доступа — https://www.inetgramotnost.ru/polezno-znat/kak-moshenniki-obretayut-dostup-k-akkauntam-polzovatelej.html (дата обращения: 02.04.2018).

17. Конфиденциальность в социальных сетях [Электронный ресурс] — Режим доступа — https://cyberleninka.ru/article/v/konfidentsialnost-v-sotsialnyh-setyah (дата обращения 06.04.2018).

18. Конфиденциальность информации в Интернете [Электронный ресурс] — Режим доступа — http://www.ripn.net/articles/privacy/ (дата обращения 06.04.2018).

19. Как защититься от взлома аккаунтов электронной почты и социальных сетей? [Электронный ресурс] — Режим доступа — http://ugolovka.com/prestupleniya/kompyuternaya-informatsiya/vzlom-akkauntov-pochty-i-sotsialnyh-setej.html (дата обращения 06.04.2018).

20. Насколько безопасно хранить свою информацию в Интернете? [Электронный ресурс] — Режим доступа — https://www.inetgramotnost.ru/polezno-znat/naskolko-bezopasno-xranit-svoyu-informaciyu-v-internete.html (дата обращения: 02.04.2018).

21. Почему люди удаляют свои аккаунты в социальных сетях? [Электронный ресурс] — Режим доступа — https://www.inetgramotnost.ru/obshhenie-v-internet/pochemu-lyudi-udalyayut-svoi-akkaunty-v-soc-setyax.html (дата обращения: 02.04.2018).

22. Понятие конфиденциальности в социальных сетях [Электронный ресурс] — Режим доступа — https://www.gcflearnfree.org/internet-safety-russian/-social/1/ (дата обращения 06.04.2018).

23. Проблемы информационной безопасности в интернет [Электронный ресурс] — Режим доступа — http://itzashita.ru/lekcii/problemy-informacionnoj-bezopasnosti-v-internet.html (дата обращения: 02.04.2018).

24. Рабочая программа по предмету «Информатика и ИКТ» для 5 — 9 классов [Электронный ресурс] — Режим доступа — https://www.школа97.екатеринбург.рф/file/download/665 (дата обращения: 02.03.2018).

25. Размещать это в социальных сетях опасно [Электронный ресурс] — Режим доступа — https://www.inetgramotnost.ru/obshhenie-v-internet/razmeshhat-eto-v-socialnyx-setyax-opasno.html (дата обращения: 02.04.2018).

26. Риски социальных сетей [Электронный ресурс] — Режим доступа — https://bezmaly.wordpress.com/2010/10/11/socialnetwork-3/ (дата обращения 06.04.2018).

27. Социальные сети как угроза корпоративной информационной безопасности [Электронный ресурс] — Режим доступа — http://www.itsec.ru/artic-les2/pravo/zaschita-personalnyh-dannyh-v-sotsialnyh-setyah (дата обращения: 02.04.2018).

28. Самозащита в социальных сетях [Электронный ресурс] — Режим доступа — https://ssd.eff.org/ru/module/самозащита-в-социальных-сетях (дата обращения 06.04.2018).

29. Угрозы социальных сетей [Электронный ресурс] — Режим доступа — http://www.itsec.ru/articles2/Inf_security/social-networks (дата обращения: 02.04.2018).

30. Michael Cross, Social Media Security [Текст] / Syngress, 2013. — 346 с. (дата обращения 02.04.2018).

31. Yuval Elovici, Yaniv Altshuler, Security and Privacy in Social Networks [Текст] / Springer Publishing Company, Incorporated, 2012. — 259 с. (дата обращения 02.04.2018).

# ПРИЛОЖЕНИЕ

**Министерство образования и науки Российской Федерации**
**Федеральное государственное автономное образовательное учреждение**
**высшего образования**
**«Российский государственный профессионально-педагогический университет»**

Институт инженерно-педагогического образования
Кафедра информационных систем и технологий
Направление подготовки 44.03.04 Профессиональное обучение (по отраслям)
Профиль «Информатика и вычислительная техника»
Профилизация «Информационная безопасность»

УТВЕРЖДАЮ
Заведующий кафедрой

_____ Н.С. Толстова
подпись и.о. фамилия

« 25 » декабря 2017 г.

**ЗАДАНИЕ**
**на выполнение выпускной квалификационной работы бакалавра**

студента (ки) *4* курса группы *ИБ-401*
***Титова Вадима Андреевича***
фамилия, имя, отчество полностью

1. Тема ***Комплекс электронных материалов «Информационная безопасность в социальных сетях»***

утверждена распоряжением по институту от «25» декабря 2017 г. № ___

2. Руководитель ***Суслова Ирина Александровна***
фамилия, имя, отчество полностью

*доцент* (ученая степень) *к.пед.н.* (ученое звание) *доцент кафедры ИС* (должность) *РГППУ* (место работы)

3. Место преддипломной практики *ФГАОУ ВО «Российский государственный профессионально-педагогический университет»*

4. Исходные данные к ВКР Michael Cross, Social Media Security
Yuval Elovici, Yaniv Altshuler, Security and Privacy in Social Networks
Безопасность в социальных сетях [Электронный ресурс]
Безопасность персональных данных в социальных сетях [Электронный ресурс]

5. Содержание текстовой части ВКР (перечень подлежащих разработке вопросов)
Анализ литературы и интернет-источников по теме «Информационная безопасность в социальных сетях»
Выбор средства реализации

Разработка структуры комплекса электронных материалов

Реализовать интерфейс комплекса электронных материалов

Реализовать видеоматериалам по различным темам и теоретический материал по темам видеоматериалов

Реализовать комплекс электронных материалов

6. Перечень демонстрационных материалов *презентация, выполненная в MS Power Point, видеоматериалы по информационной безопасности в социальных сетях*

7. Календарный план выполнения выпускной квалификационной работы

| № п/п | Наименование этапа дипломной работы | Срок выполнения этапа | Процент выполнения ВКР | Отметка руководителя о выполнении |
|---|---|---|---|---|
| 1 | Сбор информации по выпускной квалификационной работе | 23.04.2018 | 10% | |
| 2 | Выполнение работ по разрабатываемым вопросам и их изложение в пояснительной записке: | 03.05.2018 | 60% | |
| 2.1 | Анализ литературы и интернет источников | 05.05.2018 | 10% | |
| 2.2 | Анализ требований к пользовательскому интерфейсу. | 08.05.2018 | 10% | |
| 2.3 | Разработка видеоматериала по теме «Информационная безопасность в социальных сетях» | 10.05.2018 | 10% | |
| 2.4 | Проектирование структуры и реализация интерфейса, функционала, и его наполнение | 12.05.2018 | 15% | |
| 2.5 | Оптимизация мобильной версии комплекса электронных материалов | 13.05.2018 | 15% | |
| 3 | Оформление текстовой части ВКР | 15.05.2018 | 10% | |
| 4 | Выполнение демонстрационных материалов к ВКР | 01.06.2018 | 10% | |
| 5 | Нормоконтроль | 08.06.2018 | 5% | |
| 6 | Подготовка доклада к защите в ГЭК | 13.06.2018 | 5% | |

8. Консультанты по разделам выпускной квалификационной работы

| Наименование раздела | Консультант | Задание выдал | | Задание принял | |
|---|---|---|---|---|---|
| | | подпись | дата | подпись | дата |

*Руководитель* _____ _____ *Задание получил* _____ _____
подпись дата подпись студента дата

9. Дипломная работа и все материалы проанализированы.
Считаю возможным допустить ***Титова В.А.*** к защите выпускной квалификационной работы в государственной экзаменационной комиссии.
Руководитель _____ _____
подпись дата

10. Допустить ***Титова В.А.*** к защите выпускной квалификационной работы
фамилия и. о. студента
в государственной экзаменационной комиссии (протокол заседания кафедры от «___» _____ 20___г., № _____)
Заведующий кафедрой _____ _____
подпись дата